SERIE A

Cerca de la MATEMATICA (1)

Fundamentos · Algebra básica · Anexos

ADOLFO NEGRO · VALERIANO ZORIO

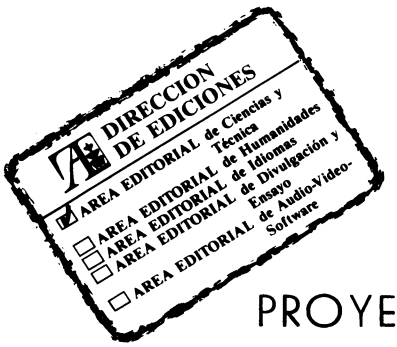
politécnica
canaima
librería
senador castillo olivares, 5
tfno.37 32 20 las palmas

PROYECTO

m62

ALHAMBRA

non scholae sed vitae discere



PROYECTO **MT-62** ALHAMBRA

COMITE EDITORIAL

Adolfo Negro

Fernando Marín Alonso

José M. Esteban

Departamentos

Coordinación, control y seguimiento
Ciencias de la Naturaleza
Ciencias de la Educación
Lengua y Literatura
Socioantropología
Matemáticas
Química
Física

CERCA DE LA MATEMATICA (1)

Fundamentos
Algebra básica
Anexos

ADOLFO NEGRO

VALERIANO ZORIO

Alhambra

Primera edición, 1975
Reimpresión, 1982
Segunda reimpresión, 1984

EDITORIAL ALHAMBRA, S.A.
R.E. 182
28001 Madrid. Claudio Coello, 76

Delegaciones:

08008 Barcelona. Enrique Granados, 61
48014 Bilbao. Iruña, 12
18009 Granada. Pza. de las Descalzas, 2
15005 La Coruña. Pasadizo de Pernas, 13
28002 Madrid. Saturnino Calleja, 1
33006 Oviedo. Avda. del Cristo, 9
38004 Santa Cruz de Tenerife. General Porlier, 14
41012 Sevilla. Reina Mercedes, 35
46003 Valencia. Cabillers, 5
50005 Zaragoza. Concepción Arenal, 25

México
Editorial Alhambra Mexicana, S.A.
Avda. División del Norte, 2412
03340 México, D.F.

n c 12040048

ISBN 84-205-0719-9 (obra completa)

ISBN 84-205-0871-3 (vol. 1)

Depósito legal: M. 40918

© Es propiedad de los autores.

Reservados todos los derechos. Ni la totalidad, ni parte de este libro pueden reproducirse o transmitirse, utilizando medios electrónicos o mecánicos, por fotocopia, grabación, información, anulado u otro sistema, sin permiso por escrito del editor.

Ilustraciones: Editorial Alhambra, S.A.
Cubierta: Editorial Alhambra, S.A.
Fotocomposición: Compoprint, S.A.
Fotomecánica: La Unión, S.A.
Impresión: Selecciones Gráficas
Papel: Kanguros
Encuadernación: Gómez Pinto, S.A.

Impreso en España - Printed in Spain

Selecciones Gráficas - Carretera de Irún, km. 11,500 - Madrid (1984)

INDICE GENERAL

Capítulos *Páginas*

1. FUNDAMENTOS

1.1 Lenguaje matemático 5

Introducción, 5. Proposiciones, 6. Razonamiento lógico. Deducción, 13. Predicados. Cuantificadores, 22. Axiomas y teoremas, 26. Inducción o recurrencia, 30. Algebra proposicional, 32. Aplicabilidad. Automatismos y destrezas, 32.

1.2 Conjuntos 37

Introducción, 37. Términos no definidos: elemento y conjunto, 38. Relación no definida: pertenencia, 38. Inclusión, 42. Identidad, 45. Operaciones conjuntistas, 48. Algebra de las partes de un conjunto. Leyes, 55. Producto cartesiano, 61. Aplicabilidad. Automatismos y destrezas, 68.

1.3 Relaciones 73

Introducción, 73. Relación binaria, 74. Relación de equivalencia, 79. Relación de orden, 84. El álgebra de las relaciones, 96. Aplicabilidad. Automatismos y destrezas, 101.

2. ALGEBRA BÁSICA

2.1 Algebra de Boole 107

Introducción, 107. Retículos. Retículos complementarios. Algebra de Boole, 108. Principio de dualidad, 111. Axiomática de Huntington para un álgebra de Boole, 111. Axiomática de Birkhoff-McLane para un álgebra de Boole, 114. Axiomática de Stoll-Goodstein para un álgebra de Boole, 116. Teoremática del álgebra de Boole, 116. El álgebra de Boole del «todo o nada», 121. Funciones booleanas, 122. Aplicabilidad. Automatismos y destrezas, 124.

2.2 Correspondencias 129

El concepto de correspondencia a partir del de relación, 129. Nomenclatura y representación, 130. Correspondencia recíproca o inversa de otra, 132. Clasificación de correspondencias. Aplicaciones, 132. Funciones: un cuadro de sinónimos, 135. Producto de correspondencias, 135. Conjunto de aplicaciones entre conjuntos finitos. Combinatoria, 143. Primera noticia de dos sugestivos conceptos: categorías y functores, 149. Aplicabilidad. Automatismos y destrezas, 150.

Capítulos *Páginas*

2.3 Ley de composición interna 155

Establecimiento, 155. Grupoide, 156. Subconjunto estable para una ley, 156. Extensión de una ley en C a $C \times C$. Estabilidad frente a una relación de equivalencia, 156. Conjunto y estructura. Acción de una operación sobre un conjunto: leyes de estructuración, 158. Un conjunto y dos leyes de composición interna: distributividad, 165. Aplicabilidad. Automatismos y destrezas, 166.

2.4 Grupos 171

Establecimiento de la estructura de grupo, 171. Grupos finitos y no finitos, 172. Creación de grupos: simetrización de semigrupos, 173. Un grupo histórico: el grupo simétrico de n variables G_n, 178. Grupos monógenos: grupos cíclicos; generadores, 184. Subgrupos, 185. El grupo de las transformaciones, 186. Conjunto cociente, módulo un subgrupo, 192. Aplicabilidad. Automatismos y destrezas, 198.

2.5 Homomorfismo 205

Establecimiento del concepto de homomorfismo, 205. Imagen homomorfa de un grupo $[A, *]$, 206. Homomorfismos canónicos o naturales, 208. Nomenclatura, 209. Equivalencia asociada a un homomorfismo, 209. Núcleo de un homomorfismo, 211. Isomorfismos de «inmersión», 212. Aplicabilidad. Automatismos y destrezas, 215.

2.6 Anillos 221

Establecimiento de la estructura de anillo, 221. Anillo de integridad; dominio de integridad, 223. Subanillos, 225. Homomorfismo en anillos, 226. Ideales, 228. Aplicabilidad. Automatismos y destrezas, 233.

2.7 Cuerpos 237

Establecimiento de la estructura de cuerpo, 237. Creación de cuerpos: simetrización en dominios de integridad, 238. Subcuerpos, 244. Ordenación en grupos, anillos y cuerpos, 246. Aplicabilidad. Automatismos y destrezas, 250.

3. ANEXOS

3.1 Conjuntos numéricos 257

El conjunto N, 257. El conjunto Z, 283. El conjunto Q, 300. Aplicabilidad. Automatismos y destrezas, 305.

3.2 Circuitos 309

Algebra de interruptores, 309. Sistema de numeración binaria, 320. Aplicabilidad. Automatismos y destrezas, 329.

3.3 Sucesos aleatorios 333

Introducción, 333. Experiencia o prueba. Sucesos elementales. Espacio muestral, 334. Conjunto-potencia de un espacio muestral, H, 335. Origen e igualdad en el conjunto $P(H)$, 336. Operaciones con números, 337. Sistema completo de sucesos, 341. Leyes del álgebra de sucesos. El álgebra de Boole de los sucesos estocásticos, 341. Aplicabilidad. Automatismos y destrezas, 343.

Capítulos *Páginas*

3.4 Frecuencia y Probabilidad 349

Introducción, 349. Experiencias reales y simuladas. Tablas de dígitos aleatorios, 351. Frecuencias absoluta y relativa, 356. Probabilidad. Modelo matemático de la frecuencia, 360. Técnica de resolución. Diez problemas resueltos, 373. Aplicabilidad. Automatismos y destrezas, 378.

3.5 Estadística 383

Introducción. Definición. Partes. Objetivos, 383. Estadística descriptiva. Distribuciones monovariantes, 384. Estadística descriptiva. Distribuciones bivariantes, 409. Distribuciones y problemas aleatorios, 422. Estadística inferencial, 438. Aplicabilidad. Automatismos y destrezas, 440.

3.6 Teoría de la información 445

Introducción, 445. La noción de información. Unidad de información, 446. Entropía de un suceso aleatorio, 448. Un ejemplo de aplicación, 450. Ordenadores, 451.

Este libro está estructurado para su utilización a dos niveles de estudio.

Los signos *y* *se disponen en los márgenes, indicando el principio y el final de las partes del texto que pueden abordarse en segunda lectura.*

1

FUNDAMENTOS

BIBLIOGRAFIA 1

PAUL LORENZEN: *Lógica formal.* Editorial Selecciones Científicas, 1970.

E. NAGEL y J. R. NEWMAN: *El teorema de Gödel.* Editorial Tecnos, 1970.

RUDOLF CARNAP: *Introduction to Symbolis Logic and its Applications.* Dover Publications Inc. 1957.

KURATOWSKI: *Introducción a la teoría de conjuntos y a la Topología.*

A. D. ALEKSANDROV, A. N. KOLMOGOROV, M. A. LAURENTIEV y otros: *La Matemática: su contenido, método y significado* (3 vols.). Alianza Editorial. Madrid, 1974.

A. TRASKI: *Introducción a la Lógica.* Espasa-Calpe. Madrid, 1968.

1.1

Lenguaje matemático

1.11. Introducción

1.12. Proposiciones

1.121. *Definición. Clases*
1.122. *Operaciones lógicas elementales*
1.123. *Tablas veritivas de Quine*
1.124. *Tautología y contradicción*

1.13. Razonamiento lógico. Deducción

1.131. *Equivalencia lógica*

1.1311. Establecimiento
1.1312. Propiedades de la equivalencia lógica
1.1313. Teorema
1.1314. Enunciados lógicamente equivalentes
1.1315. La equivalencia lógica y la conectiva bicondicional

1.132. *Implicación lógica*

1.1321. Establecimiento
1.1322. Propiedades de la implicación lógica
1.1323. La implicación lógica y la conectiva condicional

1.133. *Leyes lógicas. Deducción*

1.14. Predicados. Cuantificadores

1.141. *Predicados o funciones lógicas*
1.142. *Conjunto de validez de una función lógica*
1.143. *Cuantificador universal*
1.144. *Cuantificador existencial*
1.145. *Cuantificador existencial «exclusivo»*
1.146. *Relación entre las proposiciones universal y existencial*
1.147. *Negación de las proposiciones universal y existencial. Contraejemplo*

1.15. Axiomas y teoremas

1.151. *Introducción*
1.152. *Fases de una construcción axiomática*
1.153. *Axioma*
1.154. *Teorema*
1.155. *Condición necesaria y suficiente: proposición total*

1.16. Inducción o recurrencia

1.17. Algebra proposicional

1.18. Aplicabilidad. Automatismos y destrezas

1.1

Lenguaje matemático

1.11. INTRODUCCION

Difícil, muy difícil resulta separar la acción matemática de la expresión de ella; hasta el punto de que muchos —los llamados «formalistas»— llegan a identificar la Matemática con el lenguaje propio de su desarrollo.

Joubert dice que «buscando las palabras se encuentran las ideas». Tal vez, en su línea, se pudiera escribir en Matemáticas: cuando se expresa el hecho matemático es cuando éste existe.

Es posible que sea necesario en la etapa infantil del aprendizaje, al acercarse a la ciencia Matemática (la primogénita de las ciencias, según Leray), apoyarse en la intuición y trabajar sobre los modelos positivos que suministra el mundo natural de la materia-energía; tal vez sea necesario, pero, ciertamente, muy peligroso. La Matemática nada tiene que ver en su construcción* con la intuición.

A la hora de «escribir Matemáticas» (que es hacer Matemáticas) nada más peligroso y gratuito que esos «saltos de alfil» que el sentido común avala por correctos y que sustituyen el enfadoso rigor de la construcción lógico-matemática.

Viene a cuento aquí, la valiente frase de Vatriquat cuando escribe:

> «El sentido común, como todos los sentidos humanos, está sujeto a ilusiones y no son éstas las menos peligrosas.»

De haber presidido este espíritu el quehacer matemático de la Humanidad, posiblemente se hubieran dado menos pasos atrás y «disfrutaríamos» de menos paradojas y «agujeros» de los que aún existen y existirán en la Matemática.

---

* Decimos «en su construcción». La intuición, el don del genio, es la espléndida antorcha que ilumina a priori los problemas y caminos más ricos, al iniciar una andadura matemática; luego, aun el genio, ha de abandonarse al rigor y disciplina de un lenguaje matemático que le evite falacias y conclusiones incorrectas. Sólo en las encrucijadas, en las opciones, es donde la intuición ha de actuar, de nuevo.

Dos mil años más tarde del nacimiento de la Geometría de Euclides, Hilbert ha construido la intuición del genio griego; su elaboración es un modelo de rigor lógico deductivo. Es probable que su trabajo sea durante mucho tiempo el canon a seguir para «hacer Matemática».

Hoy se entiende que se podría escribir toda la Matemática usando tres signos lógicos y otros tres matemáticos (igualdad, pertenencia y paridad); con ellos, y «letras» a discreción, mediante una pauta de «criterios de formación» de reuniones de signos y letras, establecida a priori, se crearían las llamadas «Matemáticas formalizadas».

Salgamos al paso de un posible error: las matemáticas formalizadas no son deseables y —por supuesto— inviables, ya que, por ejemplo, conseguir en ellas crear y escribir un objeto tan simple como el número uno, en opinión de Godement, exigiría la reunión de algunas decenas de millares de signos formalizados.

No repugna en absoluto admitir que una máquina sea capaz de «hacer Matemática». Sin embargo, la idea aparente «de dioses» no deja de ser un pobre «maquinismo»: el combinar y recombinar signos y más signos, a velocidad electrónica, produciría, al azar, unas Matemáticas «inoportunas»; tal vez profundizaría hasta límites insospechados en problemas innocuos y no «atinaría» a escoger cuestiones cuyo desarrollo importa mucho al Hombre.

Déjese, pues, a los cerebros electrónicos que descarguen al Hombre de las servidumbres que él —como señor— programó; para eso han de ser. Que decidir y crear no corresponde a la máquina.

La supremacía del Hombre sobre la futurista máquina a que nos venimos refiriendo radica en el poder decidir qué reuniones de signos y letras de las formalizaciones conviene resumir, integrando nuevos objetos matemáticos o «abreviaturas», cuyas reuniones, a su vez, son los objetos con los que el Hombre libre crea y escribe sus matemáticas: las Matemáticas.

Así, pues, con el espíritu formalista, atemperado con la consciente capacidad de abreviación, se intenta hacer Matemática con un lenguaje que ha de ser

simple,
concreto,
conciso y
universal.

Para ello conviene, en principio, abordar, desde el punto de vista de la Lógica, la matematización del lenguaje usual, que es lo que se pretende en los números que siguen.

1.12. PROPOSICIONES

1.121. Definición. Clases

Se denomina proposición simple —a nuestros efectos— toda aserción verbal* de la que se puede afirmar que es falsa o cierta.

* *Con verbo.*

Ejemplo

p = «Ecuador ha suscrito el convenio "Andrés Bello" del Pacto Andino».....	p es proposición;
q = «El Ulster se anexionará a Irlanda».....	q no es proposición;
r = «2 + 3 = 7».....	r es proposición;
s = «0/0 = 4».....	s no es proposición.
«¡Deteneos, imperfectos oráculos: decidme más! Por la muerte de Sinel, sé que soy Thane de Glamis; pero ¿cómo de Cawdor?»	solamente lo subrayado es proposición.

(W. Shakespeare: *La Tragedia de Macbeth*, acto 1.º, escena III.)

Las proposiciones simples pueden conectarse entre sí, usando conjunciones (y, o, si, ni...), resultando de este modo proposiciones compuestas.

Ejemplo

p = «Sinel ha muerto.»
q = «Yo (Macbeth) soy Thane de Glamis.»
SI Sinel ha muerto, ENTONCES soy Thane de Glamis.

1.122. Operaciones lógicas elementales

Al intentar matematizar las conjunciones que producen las proposiciones compuestas por unión de otras simples se crean las siguientes operaciones lógicas elementales:

Negación: Esta operación unitaria coincide del todo con el concepto lingüístico que describe. De los múltiples signos que se usan para designarla, nosotros escogemos $\sim$, de modo que, si p es una proposición, el resultado de operar es $\sim p$, que se lee «no p» y también «es falso que p».

Ejemplo

p = «El problema palestino está resuelto»
$\sim p$ = «El problema palestino NO está resuelto»
«Es FALSO que el problema palestino esté resuelto».

(*De la Prensa diaria.*)

Disyunción: Esta operación binaria produce una proposición compuesta, mediante la conectiva «o», pero en su sentido completo de o/y. Se denota $\vee$ y se lee «o».

Ejemplo

p = «...debe ser razonable poeta»;
q = «yo sé poco del arte»;
$p \vee q$ = «...debe ser razonable poeta o yo sé poco del arte».

(M. de Cervantes: *Don Quijote de La Mancha*, cap. XXIII.)

Con las dos operaciones lógicas descritas, que llamaremos «primarias», es posible construir las restantes, siendo la más inmediata de ellas la

Conjunción: Esta operación binaria construye una proposición compuesta mediante la conectiva «y»; la signamos $\wedge$ y, en efecto, es construible con las dos primarias, de este modo:

$$p \wedge q \equiv \sim[(\sim p) \vee (\sim q)]$$

La identidad expresada se justificará en su momento.

Ejemplo

p = «...comenzaron a levantarlo en alto»;
q = «(comenzaron) a holgarse con él, como perro por carnestolendas»;
$p \wedge q$ = «... comenzaron a levantarlo en alto y a holgarse con él, como perro por carnestolendas».

(M. de Cervantes: *Don Quijote de La Mancha*, cap. XVII.)

La frase «Es falso que no comenzaron a levantarle en alto o/y a entristecerse (no holgarse) con él, como perro por carnestolendas» ciertamente no es cervantina, pero es equivalente a la del genio de la Literatura, desde un punto de vista lógico.

Como derivadas de las anteriores, describimos ahora las siguientes:

Condicional simple: Esta figura lógica responde a conectar dos proposiciones simples, mediante el modo conjuncional «si..., entonces...». La representamos por $\rightarrow$, y su construcción a partir de las operaciones primarias es

$$p \rightarrow q \equiv q \vee (\sim p)$$

(Esta identidad quedará justificada en su lugar.)

Ejemplo

p = «(Si) sospechan»;
q = «(entonces) me buscarán por el camino de París»;
$p \rightarrow q$ = «Si sospechan, me buscarán por el camino de París».

(Stendhal: *Rojo y negro*, cap. XXX.)

Bicondicional: Esta construcción lógica entre dos proposiciones las conecta mediante el modo conjuncional «si y solamente si», se denota $\leftrightarrow$ y es muy frecuente en los libros encontrar la grafía «ssi», apócope admitido del modo conjuncional registrado.

Más adelante se justificará que:

$$p \leftrightarrow q \equiv (q \vee \sim p) \wedge (p \vee \sim q)$$

Ejemplo

p = «no entrará en El»;
q = «el que no recibe el Reino de Dios como niño»;
$p \leftrightarrow q$ = «no entrará en El, si y solamente si no recibe el Reino de Dios como niño».

> «Yo os aseguro, el que no reciba el Reino de Dios como niño, no entrará en El.»
>
> (*S. Biblia*, N. T. Marcos, X, 15.)

Disyunción exclusiva: Esta operación lógica conecta dos proposiciones mediante la conjunción «o», entendida de un modo exclusivo, es decir: no contempla la acepción o/y, como lo hacía la disyunción inclusiva (simplemente, disyunción). La denotamos $\underline{\vee}$, de modo que $p \mathbin{\underline{\vee}} q$ se lee «p o q, pero no ambos».

Se justificará más adelante que la disyunción exclusiva es construible con las operaciones lógicas elementales, de esta manera:

$$p \mathbin{\underline{\vee}} q = (p \vee q) \wedge \sim(p \wedge q)$$

Ejemplo

p = «todos (somos) moros»;
q = «todos (somos) cristianos»;
$p \mathbin{\underline{\vee}} q$ = «(o) todos moros o todos cristianos».

(*Dicho popular del sudeste español.*)

Conjunción negativa: Esta conectiva lógica procede de la matematización de la contracción lingüística «y no». Es el «ni» español, y Shaffer la simboliza $\downarrow$, de modo que $p \downarrow q$ se lee «ni p ni q».

Es evidente el siguiente establecimiento lógico:

$$p \downarrow q \equiv (\sim p) \wedge (\sim q)$$

Ejemplo

p = «...no se movió de casa en toda aquella noche»;
q = «[ni] (se movió de casa) en todo el día siguiente»;
$p \downarrow q$ = «ni se movió de casa en toda aquella noche, ni en todo el día siguiente».

(G. Flaubert: *Madame Bovary*, cap. IV.)

1.123. Tablas veritivas de Quine

Quine construye unas tablas para analizar el valor de verdad de las proposiciones compuestas, a partir de los valores de verdad de las proposiciones componentes. Son éstas (signaremos por 1, proposición cierta y por 0, proposición falsa):

p	$\sim p$
1	0
0	1

Negación
El valor de verdad de la negación es el contrario al de la proposición negada.

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Disyunción
La disyunción solamente es falsa, si lo son sus dos términos.

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Conjunción
Solamente si los dos términos de la conjunción son ciertos, la conjunción es cierta.

p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Condicional simple
La condicional es siempre cierta, excepto cuando es falso *solamente* el segundo término de ella, que se llama consecuente.

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Bicondicional
La bicondicional solamente es cierta, si sus dos términos tienen el mismo valor de verdad.

p	q	$p \veebar q$
1	1	0
1	0	1
0	1	1
0	0	0

Disyunción exclusiva
La disyunción exclusiva es cierta solamente si los dos términos que la integran presentan distintos valores de verdad.

p	q	$p \downarrow q$
1	1	0
1	0	0
0	1	0
0	0	1

Conjunción negativa
La conjunción negativa solamente es cierta si son falsos los dos términos que la constituyen.

Se pueden construir proposiciones más complejas conectando con las conectivas descritas varias proposiciones de las que venimos expresando, tales son los dos ejemplos que se escriben:

$$\sim(p \wedge \sim q)$$
$$[\sim p \rightarrow (q \rightarrow r)] \vee (p \leftrightarrow r)$$

Para abordar la determinación del valor de verdad de esas proposiciones, existen dos métodos o técnicas: el método acumulativo y el método por pasos. El primero es adecuado para las proposiciones no excesivamente complicadas, como puede ser el primer ejemplo propuesto; el método por pasos es el indicado para la segunda proposición compuesta, ya que es suficientemente compleja para intentar el primer método, que resultaría largo y engorroso.

Procedemos a determinar el valor de verdad de los dos ejemplos propuestos.

Método acumulativo: El análisis ha de proceder «de dentro a fuera».

1. Se describen las dos primeras columnas con todos los posibles valores de verdad de las proposiciones simples p y q.
2. Se analiza $\sim q$.
3. Se analiza $p \wedge \sim q$.
4. Se acaba con el análisis $\sim(p \wedge \sim q)$.

p	q	$\sim q$	$p \wedge \sim q$	$\sim(p \wedge \sim q)$
1	1	0	0	1
1	0	1	1	0
0	1	0	0	1
0	0	1	0	1

Método de pasos:

1. Se disponen las tres primeras columnas (en este ejemplo hay tres proposiciones simples: p, q y r) con todos los posibles valores de verdad de las proposiciones simples.
2. Se escribe en cabecera de tabla la proposición a analizar, procurando separar convenientemente cada uno de sus símbolos.
3. Se dispone en cola de tabla un casillero, para registrar el orden de los pasos a dar.
4. Como siempre, «de dentro a fuera», se realizan los análisis parciales de la proposición, constituyendo siempre los primeros pasos la transcripción de los valores de verdad de las proposiciones simples.
5. La columna que ostente el número de paso más elevado registrará el valor de verdad de la proposición analizada.

p	q	r	$\sim$	$[p$	$\rightarrow$	$(q$	$\rightarrow$	$r)]$	$\vee$	$(p$	$\leftrightarrow$	$r)$
1	1	1	0	1	1	1	1	1	1	1	1	1
1	0	1	0	1	1	0	1	1	1	1	1	1
0	1	1	0	0	1	1	1	1	0	0	0	1
0	0	1	0	0	1	0	1	1	0	0	0	1
1	1	0	1	1	0	1	0	0	1	1	0	0
1	0	0	0	1	1	0	1	0	0	1	0	0
0	1	0	0	0	1	1	0	0	1	0	1	0
0	0	0	0	0	1	0	1	0	1	0	1	0
Pasos			4.º	1.º	3.º	1.º	2.º	1.º	5.º	1.º	2.º	1.º

Adviértase que todos los análisis del valor de verdad de las proposiciones que se vienen realizando se llevan a cabo sobre las expresiones generales de las mismas, sin descender a los enunciados concretos a que puedan referirse. Esto es sumamente importante y es, precisamente, lo que le da calidad matemática al método. Interesa poco que los contenidos de la proposición analizada se refieran a un planteamiento político o a una disquisición sobre deportes; lo que importa es la estructura formal lógica de la proposición analizada.

Insistiendo sobre el primer ejemplo que hemos analizado, a la vista del resultado de su tabla de verdad, se puede asegurar que la proposición compuesta —se refiera al tema que se refiera— resulta ser siempre cierta, excepto cuando la proposición p lo es, no siéndolo la q.

1.124. Tautología y contradicción

Se denomina tautología una proposición que es cierta para cualquier valor de verdad de sus componentes.

Es claro, entonces, que en su tabla veritiva «la última columna» estará formada por 1. La signaremos por una «uve» mayúscula, V.

Contradicción es la negación de una tautología; por tanto, una proposición que es falsa para cualquier valor de verdad de sus componentes es una proposición contradictoria o *absurdo*.

Naturalmente, al analizar el valor de verdad de un absurdo, la última columna de su tabla arrojará todos 0. Lo denotaremos por una «efe» mayúscula, *F*.

Ejemplo

Tautología

p	p	$\vee$	$\sim$	p
1	1	1	0	1
0	0	1	1	0

Contradicción

p	p	$\wedge$	$\sim$	p
1	1	0	0	1
0	0	0	1	0

Enunciados lógicamente verdaderos: Suelen recibir ese nombre los enunciados concretos (frases de contenido específico) que proceden de una tautología.

Ejemplo

El enunciado genético

«Un animal sexuado es macho o es hembra»

es un enunciado lógicamente verdadero, ya que su estructura lógica es la tautología $p \vee \sim p$.

(Tal vez, «adivinamos» la extrañeza de algún lector que, pensando en el hermafroditismo, entiende que el enunciado propuesto no es tautológico. Recuerde que la disyunción planteada no es la exclusiva y, por tanto, abarca el caso o/y:

1.13. RAZONAMIENTO LOGICO. DEDUCCION

Hasta el momento, hemos conseguido crear dos cosas: de un lado, los objetos matemáticos, llamados proposiciones; de otro, las operaciones lógicas fundamentales sobre ellos: negación, disyunción y conjunción.

Nos quedan por establecer otras dos, para que podamos hacer matemáticas: la equivalencia lógica y la implicación lógica. Con ello, habremos introducido la relación de igualdad y la relación de orden, factores ineludibles en todo tratamiento matemático completo.

Al borde de la teoría del conocimiento, el concepto de equivalencia lógica no es más (¡ni menos!) que el vidrioso tema de la identidad, el profundo concepto

de igualdad; la implicación lógica es una relación* entre los objetos lógicos, instrumento que permite el razonamiento deductivo.

1.131. Equivalencia lógica

1.1311. *Establecimiento*

Sean las proposiciones $P(p, q, \ldots)$ y $Q(p, q, \ldots)$, indicando con esta notación que pueden ser proposiciones compuestas de las simples $p, q, \ldots$

Se dice que dos proposiciones son lógicamente equivalentes, si sus tablas de verdad coinciden. Usando el signo $\Leftrightarrow$, escribimos:

$$P(p, q, \ldots) \Leftrightarrow Q(p, q, \ldots)$$

Ejercicio-ejemplo

A lo largo del 1.122 se ha dado noticia de equivalencias lógicas, usando en lugar del signo $\Leftrightarrow$, el menos específico $\equiv$.

Ahora debe comprobarse que son equivalencias lógicas, estableciendo sus tablas de verdad, las que se recopilan a continuación:

$$p \wedge q \Leftrightarrow \sim[(\sim p) \vee (\sim q)]$$
$$p \rightarrow q \Leftrightarrow q \vee (\sim p)$$
$$p \leftrightarrow q \Leftrightarrow (q \vee \sim p) \wedge (p \vee \sim q)$$
$$p \veebar q \Leftrightarrow (p \vee q) \wedge \sim(p \wedge q)$$
$$p \downarrow q \Leftrightarrow (\sim p) \wedge (\sim q)$$

1.1312. *Propiedades de la equivalencia lógica*

La equivalencia lógica es una relación reflexiva, simétrica y transitiva. En efecto:

Reflexividad: $P \Leftrightarrow P$

Toda proposición tiene la misma tabla de verdad que ella misma.

Simetría: $(P \Leftrightarrow Q) \rightarrow (Q \Leftrightarrow P)$

Si una proposición tiene la misma tabla de verdad que otra, ésta la tiene coincidente con la de la primera.

Transitividad: $[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \rightarrow (P \Leftrightarrow R)$

Si la tabla de verdad de P es igual a la de Q, y la de ésta coincide con la de R, entonces P y R tienen tablas de verdad coincidentes.

---

* Inevitablemente, hemos de escribir términos que, por no establecidos, todavía son gratuitos o improcedentes, desde un punto de vista de secuencialización lógico-matemática. Sin embargo, confiamos en que el lector no se ha de escandalizar, ya que, según los casos, tendrá la discreción (bien consciente, bien por falta de ciencia) de tomar los términos en la acepción usual o matematizados.

Por tanto, como —sin duda— conoce el lector de su aprendizaje anterior, la equivalencia lógica, al poseer estas tres propiedades, es una relación de equivalencia.

1.1313. TEOREMA *:

La condición necesaria y suficiente para que dos proposiciones sean lógicamente equivalentes es que su bicondicional sea tautológica.

En efecto: si P y Q, por ser lógicamente equivalentes, tienen tablas de verdad idénticas, la bicondicional $P \leftrightarrow Q$ «conecta» entre sí valores de verdad iguales y, según su tabla, produce siempre 1; luego

es condición necesaria.

Si la bicondicional $P \leftrightarrow Q$ es una tautología es porque los valores de verdad de P y de Q que «conecta» son siempre iguales (véase tabla); es decir, P y Q son lógicamente equivalentes; o sea:

es condición suficiente.

(Si resulta demasiado «literaria» la exposición, comprenda el lector que aún no tenemos derecho a utilizar la implicación lógica, que matematizaría el formalismo.)

COROLARIO: Dos tautologías o dos contradicciones son siempre lógicamente equivalentes.

1.1314. *Enunciados lógicamente equivalentes*

Reciben este nombre los enunciados concretos cuyas formas proposicionales son lógicamente equivalentes.

Ejemplo

«Ni tú velas, ni yo duermo» $p \downarrow q$
«Tú no velas y yo no duermo» $(\sim p) \wedge (\sim q)$

Los dos enunciados son lógicamente equivalentes, ya que

$$(p \downarrow q) \Leftrightarrow [(\sim p) \wedge (\sim q)]$$

1.1315. *La equivalencia lógica y la conectiva bicondicional*

Es lamentablemente frecuente encontrar confusionismo en el uso de los signos $\Leftrightarrow$ y $\leftrightarrow$. Quede dicho, de una vez por todas, que representan conceptos absolutamente distintos y que no es lícito su uso indiscriminado.

---

* De nuevo advertimos que quebramos la secuencia lógica de la exposición, en favor de un «orden didáctico». La expresión eminentemente teoremática que sigue es aquí gratuita en puridad lógica, pues no se podría abordar de este modo hasta que no se hubiera concluido la exposición del razonamiento deductivo. Tomamos la decisión de entender al lector, informado «de alguna manera» en sus aprendizajes elementales, y ahorrarle el durísimo camino de una exposición rigurosamente formalizada y secuencializada.

Siendo P y Q dos proposiciones, $P \leftrightarrow Q$ también lo es y, como tal, su tabla de verdad tendrá «ceros» o «unos», en función de los valores de verdad de sus componentes; mientras que $P \Leftrightarrow Q$ no es una proposición, sino una relación entre proposiciones.

Lo que sucede —y de ahí el confusionismo— es que, como se acaba de ver, la relación de equivalencia lógica exige que la bicondicional entre las proposiciones equivalentes sea una tautología, de modo que en este caso la bicondicional $P \leftrightarrow Q$, «asociada a la equivalencia», tiene todo «unos» en su tabla de verdad. Tal es así, que muchos lógicos no admiten distinción alguna entre dos proposiciones equivalentes y sustituyen el signo $\Leftrightarrow$ por el $=$.

1.132. Implicación lógica

1.1321. *Establecimiento*

Se dice que una proposición P implica lógicamente otra Q, y escribimos

$$P \Rightarrow Q,$$

si, y solamente si, la condicional de la segunda a la primera* es tautológica:

$$P \rightarrow Q \text{ es tautología.}$$

Ahora ya podemos simbolizar la equivalencia lógica (la identidad) de esas dos proposiciones

$$(P \Rightarrow Q) \Leftrightarrow [(P \rightarrow Q) \equiv V]$$

Teniendo en cuenta que las proposiciones

$$\begin{aligned} &P \rightarrow Q \text{ es tautología,} \\ &P \wedge \sim Q \text{ es contradicción y} \\ \sim P \vee &Q \text{ es tautología} \end{aligned}$$

son lógicamente equivalentes, se pueden usar cualquiera de las tres para «descubrir» si una proposición P implica otra Q.

1.1322. *Propiedades de la implicación lógica*

La implicación lógica es una relación reflexiva, antisimétrica y transitiva. En efecto:

---

* Efectivamente, se ha querido escribir «de la segunda a la primera», que es la forma correcta de decir que P es condición para Q: $(P \rightarrow Q)$.

Reflexividad: $P \Rightarrow P$

La condicional $P \rightarrow P$ es tautológica por «conectar» siempre valores de verdad idénticos.

Antisimetría: $[(P \Rightarrow Q) \wedge (Q \Rightarrow P)] \rightarrow (P \Leftrightarrow Q)$

Se lee: si P implica Q y Q implica P, entonces P es equivalente a Q (P es Q).
La única forma de que se impliquen mutuamente es que tengan iguales tablas de verdad, o sea, que sean equivalentes.

Transitividad: $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \rightarrow (P \Rightarrow R)$

Bástenos por ahora decir que es evidente, aunque con la conciencia de que esa «evidencia» no justifica nada. Sí lo harán, sin embargo, posteriores establecimientos.

Como recordará el lector de sus aprendizajes anteriores, una relación con estas propiedades es una relación de orden.

1.1323. *La implicación lógica y la conectiva condicional*

No han de confundirse los signos $\rightarrow$ y $\Rightarrow$, pues responden a dos conceptos muy diferentes.

Si P y Q son dos proposiciones, la condicional $P \rightarrow Q$ lo sigue siendo, de modo que su tabla de verdad arrojará «ceros» o «unos», según los valores de verdad de las componentes P y Q.

La expresión $P \Rightarrow Q$ es una relación (de orden) entre proposiciones. Sucede que asociada a la implicación lógica está la condicional tautológica $P \rightarrow Q$, cuya tabla de verdad, consecuentemente, ha de estar formada exclusivamente por «unos».

Escribir $P \rightarrow Q$, es establecer una condicional que, tras su análisis, resultará cierta o falsa, según los casos; afirmar que $P \Rightarrow Q$, exige que $P \rightarrow Q$ sea siempre verdadera.

1.133. Leyes lógicas. Deducción

El modo más «universal» del trabajo matemático es la deducción lógico-matemática. Consiste en esencia en, arrancando de unas proposiciones que se admiten como ciertas, denominadas *premisas*, llegar mediante una cadena de implicaciones lógicas a una proposición final, llamada *conclusión*.

El conjunto de premisas constituye la *hipótesis* y la conclusión es la *tesis*. La cadena de implicaciones lógicas, lícitas, que permiten pasar de la hipótesis a la tesis recibe el nombre de *demostración*.

Se denomina *teorema* a todo el conjunto lógico-matemático que se ha descrito.

Para que la cadena de implicaciones lógicas que constituyen la demostración sea lícita ha de obedecer a un principio y a una serie de leyes, de las cuales pasamos a exponer las de más frecuente uso.

Téngase en cuenta que es posible establecer tantas leyes lógicas formales como tautologías proposicionales pueden escribirse, pues, precisamente, la autoridad de estas leyes radica en su validez universal (tautológica).

P_0) *Principio de sustitución*

Si se dispone de una proposición tautológica $P(p, q, \ldots)$, y se sustituyen en ella sus proposiciones componentes por otras, la proposición resultante, $P, (p', q', \ldots)$, sigue siendo una tautología.

Ejemplo

Sea la tautología $(p \wedge q) \to p$. Si se sustituye en ella

$$\begin{array}{l} p \text{ por } (r \to t) \\ q \text{ por } t, \end{array}$$

la proposición

$$[(r \to t) \wedge t] \to (r \to t)$$

es tautológica.

Para mostrarlo, basta realizar la tabla de verdad de ambas.

A_1) *Ley de absorción*

$$p \vee (p \wedge q) \Leftrightarrow p \quad ; \quad p \wedge (p \vee q) \Leftrightarrow p$$

A_2) *Ley de idempotencia*

$$p \vee p \Leftrightarrow p \quad ; \quad p \wedge p \Leftrightarrow p$$

A_3) *Ley de asociatividad*

$$[(p \vee q) \vee r] \Leftrightarrow [p \vee (q \vee r)] \quad ; \quad [(p \wedge q) \wedge r] \Leftrightarrow [p \wedge (q \wedge r)]$$
$$[(p \leftrightarrow q) \leftrightarrow r] \Leftrightarrow [p \leftrightarrow (q \leftrightarrow r)]$$

A_4) *Ley de conmutatividad*

$$(p \vee q) \Leftrightarrow (q \vee p) \quad ; \quad (p \wedge q) \Leftrightarrow (q \wedge p)$$

A_5) *Ley de complementariedad*

$$p \vee \sim p \Leftrightarrow V \quad ; \quad p \wedge \sim p \Leftrightarrow F$$
(ley del tercero excluido) (ley de contradicción)

A_6) *Ley de distributividad*

$$[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \vee (p \vee r)]$$
$$[p \wedge (q \vee r)] \Leftrightarrow [(p \wedge q) \vee (p \wedge r)]$$
$$[p \to (q \vee r)] \Leftrightarrow [(p \to q) \vee (p \to r)]$$
$$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$$

T_7) *Ley de identidad* (cotas universales)

$$(p \vee F) \Leftrightarrow p \quad ; \quad (p \wedge V) \Leftrightarrow p$$

T_8) *Ley de involución* (doble negación)

$$\sim(\sim p) \Leftrightarrow p$$

T_9) *Ley de De Morgan*

$$\sim(p \vee q) \Leftrightarrow [(\sim p) \wedge (\sim q)] \quad ; \quad \sim(p \wedge q) \Leftrightarrow [(\sim p) \vee (\sim q)]$$

T_{10}) *Ley de simplificación*

$$p \Rightarrow (p \vee q) \quad ; \quad (p \wedge q) \Rightarrow p$$

T_{11}) *Ley de transitividad* (silogismo hipotético)

$$[(p \to q) \wedge (q \to r)] \Rightarrow (p \to r)$$
$$[(p \leftrightarrow q) \wedge (q \leftrightarrow r)] \Rightarrow (p \leftrightarrow r)$$

T_{12}) *Ley del dilema* (silogismo disyuntivo)

$$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \Rightarrow (q \vee s)$$

T_{13}) *Ley bicondicional*

$$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$$

T_{14}) *Ley condicional*

$(p \to q) \Leftrightarrow (\sim p \vee q)$; $(p \to q) \Leftrightarrow \sim(p \wedge \sim q)$
(condicional disyuntiva) (reducción al absurdo)

T_{15}) *Ley de transposición*

$$(p \to q) \Leftrightarrow (\sim q \to \sim p)$$
$$(p \leftrightarrow q) \Leftrightarrow (\sim p \leftrightarrow \sim q)$$

T_{16}) *Ley de exportación*

$$[(p \wedge q) \to r] \Leftrightarrow [p \to (q \to r)]$$

T_{17}) *Ley de expansión*

$$(p \to q) \Leftrightarrow [(p \vee q) \leftrightarrow q]$$
$$(p \leftrightarrow q) \Leftrightarrow [(p \wedge q) \leftrightarrow p]$$

T_{18}) *Ley de separación (modus ponendo ponens)*

$$[(p \to q) \wedge p] \Rightarrow q$$

T_{19}) *Ley «modus tollendo tollens»*

$$[(p \to q) \wedge \sim q] \Rightarrow \sim p$$

T_{20}) *Ley «modus tollendo ponens»*

$$[(p \vee q) \wedge \sim p] \Rightarrow q$$

Tal vez se haya observado que a partir de la séptima ley se ha escrito T en lugar de A; ello obedece a una intencionalidad de diferenciación entre esos dos bloques, para posteriores desarrollos (A = axioma; T = teorema).

Cualesquiera de las leyes establecidas pueden justificarse universalmente válidas, realizando las tablas de verdad de sus condicionales o bicondicionales asociadas*, que en todos los casos resultarán ser tautologías.

A continuación se facilita el análisis de un razonamiento sobre enunciados concretos, explicitando las leyes en que se basa y concluyendo su corrección o incorrección lógicas.

Ejemplo

Si la inflación existe, entonces los precios son abusivos. La inflación existe y tiene ámbito mundial. Si los precios son exagerados, no se tiene poder de adquisición. Se puede asegurar, pues, que la inflación prohíbe el consumo.

A) *Establecimiento de las proposiciones*

p = «La inflación existe»;
q = «Los precios son abusivos»;
r = «La inflación tiene ámbito mundial»;
s = «Se tiene $\begin{cases} \text{poder de adquisición»;} \\ \text{posibilidad de consumo».} \end{cases}$

B) *Establecimiento de las premisas y de la conclusión*

$$\left.\begin{array}{l} \text{Primera premisa: } p \to q \\ \text{Segunda premisa: } p \wedge r \\ \text{Tercera premisa: } q \to \sim s \end{array}\right\} \text{Hipótesis: } [(p \to q) \wedge (p \wedge r) \wedge (q \to \sim s)]$$
$$\text{Conclusión: } \sim s \qquad \text{Tesis: } \sim s$$

---

* Recuérdese que $P \Leftrightarrow Q$ si, y solamente si, $P \leftrightarrow Q$ es tautología; y que $P \Rightarrow Q$ si, y solamente si, $P \to Q$ es tautología.

C) *Establecimiento del razonamiento*

$$[(p \to q) \wedge (p \wedge r) \wedge (q \to \sim s)] \Rightarrow \sim s$$

D) *Análisis del razonamiento*

Puede realizarse un análisis proposicional o bien una deducción lógica. Suministramos las dos cosas.

El razonamiento será correcto si la condicional asociada a su implicación es tautológica, o sea:

$$([p \to q) \wedge (p \wedge r) \wedge (q \to \sim s)] \to \sim s) \equiv V$$

Veamos:

p	q	r	s	$[(p$	$\to$	$q)$	$\wedge$	$(p$	$\wedge$	$r)$	$\wedge$	$(q$	$\to$	$\sim$	$s)]$	$\to$	$\sim$	s
1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	1	0	1
1	0	1	1	1	0	0	0	1	1	1	0	0	1	0	1	1	0	1
0	1	1	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	1
0	0	1	1	0	1	0	0	0	0	1	0	0	1	0	1	1	0	1
1	1	0	1	1	1	1	1	1	0	0	0	1	0	0	1	1	0	1
1	0	0	1	1	0	0	0	1	0	0	0	0	1	0	1	1	0	1
0	1	0	1	0	1	1	0	0	0	0	0	1	0	0	1	1	0	1
0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	1	1	0	1
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0
1	0	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1	1	0
0	1	1	0	0	1	1	0	0	0	1	0	1	1	1	0	1	1	0
0	0	1	0	0	1	0	0	0	0	1	0	0	1	1	0	1	1	0
1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	0	1	1	0
1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	0	1	1	0
0	1	0	0	0	1	1	0	0	0	0	0	1	1	1	0	1	1	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	1	1	0
Pasos				1.º	2.º	1.º	**4.º**	1.º	2.º	1.º	**5.º**	1.º	3.º	2.º	1.º	**6.º**	2.º	1.º

Deducciòn lògica

Hipótesis:

$$[(p \to q) \wedge (p \wedge r) \wedge (q \to \sim s)]$$
$$\Updownarrow \quad \text{por } A_4$$
$$[(p \to q) \wedge (q \to \sim s) \wedge (p \wedge r)]$$
$$\Downarrow \quad \text{por } T_{11} \text{ y } P_0$$
$$[(p \to \sim s) \wedge (p \wedge r)]$$
$$\Downarrow \quad \text{por } T_{10} \text{ y } P_0$$
$$[(p \to \sim s) \wedge p]$$
$$\Downarrow \quad \text{por } T_{18}$$
$$\sim s$$

1.14. PREDICADOS. CUANTIFICADORES

1.141. Predicados o funciones lógicas

Sea p un enunciado formal y A un conjunto. Función lógica sobre A es toda expresión

$$p(x),$$

que especificada para cualquier elemento a de A, hace que $p(a)$ sea una proposición falsa o cierta.

Ejemplo

Sea el enunciado formal p = «x es número par», y sea $A = \{1, 2, 3, 4\}$. Son predicados sobre A todos los $p(x)$, $x \in A$, pues su valor de verdad es decidible:

$p(1)$ = «1 es un número par»; predicado falso: (0)
$p(2)$ = «2 es un número par»; predicado cierto: (1)
$p(3)$ = «3 es un número par»; predicado falso: (0)
$p(4)$ = «4 es un número par»; predicado cierto: (1)

Pueden haber funciones lógicas $p(x, y)$ en dos o más variables, sobre los elementos de un conjunto A

Ejemplo

p = «x divide a y»; $A = \{2, 3, 6, 4, 12\}$

$p(2, 3)$ es predicado (0)
$p(2, 6)$ es predicado (1)
$p(12, 6)$ es predicado (0)
$p(6, 12)$ es predicado (1), etc.

Además, las funciones lógicas pueden conectarse entre sí, usando las conectivas proposicionales, resultando, de este modo, predicados más complejos.

1.142. Conjunto de validez de una función lógica

Sea $p(x)$ un predicado sobre A. El conjunto de elementos de A para los que $p(x)$ es cierta se denomina conjunto de validez de $p(x)$ sobre A. Lo denotamos $A_{[1]}$, de modo que

$$A_{[1]} = \{x/(x \in A) \wedge (p(x) \text{ es cierto})\}^*$$

---

* Otra vez, en favor de la didáctica, entendemos que el lector, procedente de aprendizajes medios, no tendrá dificultad en comprender la expresión conjuntista.

Ejemplo 1

El conjunto de validez de p = «x es número par» sobre $A = \{1, 2, 3, 4\}$ es

$$A_{[1]} = \{2, 4\}$$

Ejemplo 2

Si p = «x es negativo» y N es el conjunto de los números naturales, el predicado $p(x)$ sobre N tiene como conjunto de validez, el conjunto vacío

$$N_{[1]} = \phi$$

Ejemplo 3

Si p = «x es primo» y es $A = \{1, 2, 3, 5, 7, 11\}$, el predicado $p(x)$ sobre A tiene de conjunto de validez el propio A

$$A_{[1]} = A$$

Ejemplo 4

Si p = «x es primo» y $A = \{10, 13, 15, 20\}$. El predicado $p(x)$ sobre A tiene de conjunto de validez el conjunto unitario $A_{[1]} = \{13\}$.

Se habrá venido observando en los ejemplos anteriores que la función lógica, $p(x)$, definida sobre un conjunto A, puede ser cierta

para todos los elementos de A;
para algunos elementos de A;
para un solo elemento de A o
para ningún elemento de A.

1.143. Cuantificador universal

Considérese la función lógica $p(x)$ sobre un conjunto A, y sea su conjunto de validez $A_{[1]} = A$; es decir, que p es cierta *para todo* $x \in A$. Pues bien: el símbolo $\forall$ se llama cuantificador universal y se lee «para todo», de modo que

$$\forall x \in A,\ p(x) \qquad [1]$$

se lee: «para todo elemento x de A es cierto p».

Adviértase que, mientras que $p(x)$ es una función lógica, la expresión [1] ya es una proposición, con su correspondiente valor de verdad. Es la llamada *proposición universal.*

Tras lo dicho, queda claro que para que una proposición universal sea cierta es necesario y suficiente que el conjunto de validez de su función lógica coincida con su conjunto de definición. Simbólicamente:

$$[\forall x \in A,\ p(x)] \Leftrightarrow [A_{[1]} \equiv A]$$

Ejemplo 1

Enunciado formal: p = «x es par o impar, pero no ambas cosas».
Conjunto de definición: conjunto de los números naturales, N.
La proposición universal

«Todo número natural es par o impar, pero no ambas cosas», que se simboliza

$$\forall x \in N,\ [(x = \dot{2}) \veebar (x = \dot{2} + 1)],$$

es cierta, pues el $N_{[1]}$ de p coincide con N.

Ejemplo 2

La proposición universal

$$\forall x \in N,\ (x = \dot{5})$$

es falsa, pues $N_{[1]} \neq N$.

1.144. Cuantificador existencial

Sea la función lógica $p(x)$ sobre un conjunto A, y sea su conjunto de validez $A_{[1]}$, formado por alguno, algunos o todos los elementos de A; es decir, que $p(x)$ es cierta *al menos* para un $x \in A$.

Pues bien: el símbolo $\exists$ se llama cuantificador existencial y se lee «existe al menos uno», de modo que

$$\exists x \in A,\ p(x) \qquad [2]$$

es la llamada *proposición existencial*, que significa:

«existe al menos un elemento de A, para el que p es cierta».

Como anteriormente, mientras $p(x)$ es función lógica, la expresión [2] ya es una proposición, con el correspondiente valor de verdad.

Es claro que para que una proposición existencial sea cierta es necesario y suficiente que el conjunto de validez de su función lógica tenga algún elemento. O sea:

$$[\exists x \in A,\ p(x)] \Leftrightarrow [A_{[1]} \neq \phi]$$

Ejemplo

Función lógica: p = «x es líquido».
Conjunto de definición: M = {los metales}.

La proposición existencial:

«Existe al menos un metal que es líquido»,

que se simboliza:

$$\exists x \in M,\ x \text{ es líquido},$$

es cierta, pues $M_{[1]} = \{\text{Hg}\} \neq \phi$.

1.145. Cuantificador existencial «exclusivo»

Si el conjunto de validez de una función lógica es unitario, el cuantificador existencial que la transforma en proposición puede ser el descrito

$$\exists = \text{«existe al menos uno»},$$

o podemos introducir una «abreviatura» más «robusta»,

$$\exists^* = \text{«existe uno y solamente uno»},$$

que exige más que la anterior.

Es muy frecuente su uso en álgebra de funciones.

Ejemplo

«Para cada par de naturales existe un solo natural, que es su suma».
Función lógica: $x + y = z$.
Conjunto de definición: N.
Proposición existencial: $\exists^* z \in N,\ x + y = z$.

1.146. Relación entre las proposiciones universal y existencial

Brindamos al análisis del lector la equivalencia lógica

$$\sim[\exists x,\ \sim p] \Leftrightarrow [\forall x,\ p]$$

entre ambas proposiciones cuantificacionales.

El análisis proposicional justifica la corrección de la equivalencia establecida.

Ejemplo

p = «x es mortal».
Conjunto de definición: H = {género humano}.
$\sim[\exists x,\ \sim p]$ = «Es falso que exista al menos un hombre que no sea mortal».
$[\forall x,\ p]$ = «Todo hombre es mortal».

NOTA. Adviértase que si para un p sobre A, su conjunto de validez es $A_{[1]}$, el conjunto de validez de $\sim p$ es el complementario de $A_{[1]}$ en A.

1.147. Negación de las proposiciones universal y existencial. Contraejemplo

Con el nombre de teoremas de De Morgan se conocen las dos siguientes equivalencias lógicas, cuyos análisis proposicionales las justifican como correctas:

$$[\sim(\forall x,\ p)] \Leftrightarrow [\exists x,\ \sim p] \qquad [1]$$

$$\sim(\exists x,\ p) \Leftrightarrow [\forall x,\ \sim p] \qquad [2]$$

Contraejemplo

Muy usada en Matemáticas la técnica del contraejemplo, es el método para demostrar la negación de una proposición universal.

Basándonos en la equivalencia lógica [1] de De Morgan, si se trata de justificar la primera proposición, bastará con demostrar la segunda, es decir, que existe al menos un x para el que es falsa p. Pues bien: ese x_0, tal que $p(x)$ es falso, es lo que se llama contraejemplo de la proposición universal $(\forall x,\ p)$.

Ejemplo

Demuéstrese que es falso que el cuadrado de todo número real es mayor que la base. O sea:

$$\sim[\forall x \in R,\ x^2 > x]$$

Basta justificar que

$$\exists x \in R,\ x^2 \not> x,$$

para lo cual es suficiente establecer el contraejemplo $1/3 \in R$, pues

$$(1/3)^2 \not> 1/3$$

1.15. AXIOMAS Y TEOREMAS

1.151. Introducción

Una ciencia comienza a serlo cuando ha superado su fase enciclopédica de acumulación de noticias y tratamientos individualizados en departamentos-estanco de sus diferentes parcelas, y evidencia la exigencia de un edificio único, conexo, en que nada es «isla» y todo encaja en su lugar, como pieza inexcusable de la estructura científica.

En ese momento, multitud de cuestiones se denuncian como inútiles, aparecen duplicados y triplicados tratamientos que, con formas aparentemente independien-

tes, en el fondo no son más que concreciones de una única teoría general. Y también —digámoslo— aparecen los «fantasmas» de toda ciencia: las paradojas y contradicciones. Entonces se hace inevitable la rigurosa construcción axiomatizada de todo el edificio científico.

1.152. Fases de una construcción axiomática

El desarrollo axiomático de una determinada teoría tiene tres fases:

Primera. Establecimiento de los términos no definidos.

Han de fijarse unos conceptos básicos, primarios al hombre, que no admiten definición.

Segunda. Determinación de relaciones no definidas.

Con la misma esencia anterior, son relaciones que el hombre pone en la base de su conocimiento.

Tercera. Postular* los axiomas que relacionan entre sí los términos no definidos con las relaciones no definidas.

Establecidas las tres fases que anteceden, se comienza a construir el cuerpo de ciencia: la teoremática, conjunto de proposiciones a demostrar como ciertas.

A continuación, disponemos un cuadro-ejemplo, en el que se escriben algunos de los términos de los desarrollos axiomáticos de dos teorías matemáticas bien conocidas: la Geometría de Euclides y la Teoría de Conjuntos.

	Geometría euclídea	*Teoría de Conjuntos*
Términos no definidos	punto recta plano	elemento conjunto
Relaciones no definidas	punto en recta recta en plano	pertenencia
Axiomas	Dos puntos determinan una recta. Por un punto exterior a una recta sólo existe una paralela a ella.	$(A \cup B) \cap A = A$ $A \cup \phi = A$ $A \cap U = A$

* Del latín *postulare* = pedir.

1.153. Axioma o postulado es una proposición que se admite como cierta.

Para construir un desarrollo axiomático se ha de partir de un conjunto o sistema de axiomas, escogidos arbitrariamente, que ha de ser

— compatible,
— suficiente e
— independiente.

Compatibilidad: dos axiomas no pueden postular en ellos, ni producir en sus teoremas relaciones contradictorias;

Suficiencia: toda proposición teoremática ha de ser deducible dentro del sistema;

Independencia: ningún axioma ha de poderse deducir de otros.

Establecido el sistema de axiomas (que, por cierto, no tienen por qué ser «evidentes» (!)), se comienza a construir, enunciando y demostrando los teoremas.

1.154. Teorema es una proposición que ha de demostrarse cierta, mediante un razonamiento lógico, a partir de los axiomas o de otros teoremas, previamente justificados.

Un teorema tiene tres partes:

Hipótesis: es la conjunción de las premisas del razonamiento lógico. Está constituida por axiomas o por proposiciones teoremáticas, previamente justificadas como ciertas;

Tesis: es la proposición conclusiva del razonamiento lógico;

Demostración: es la cadena de implicaciones lógicas, lícitas, que llevan desde la hipótesis hasta la tesis.

Establecido como *directo* el teorema formal $H \Rightarrow T$, se denomina *recíproco* de él el que invierte la hipótesis y la tesis: $T \Rightarrow H$.

Ejemplo

Directo: Si $P(a) = 0$, entonces $P(x) = \dot{\overline{x - a}}$.
Recíproco: Si $P(x) = \dot{\overline{x - a}}$, entonces $P(a) = 0$.

Teorema *contrario* de otro es el que niega la hipótesis y la tesis del directo: $\sim H \Rightarrow \sim T$.

Ejemplo

Directo: Si $P(a) = 0$, entonces $P(x) = \dot{\overline{x - a}}$.
Contrario: Si $P(a) \neq 0$, entonces $P(x) \neq \dot{\overline{x - a}}$.

El teorema *contrarrecíproco* de otro, considerado como directo, es aquel que invierte y niega la hipótesis y la tesis: $\sim T \Rightarrow \sim H$.

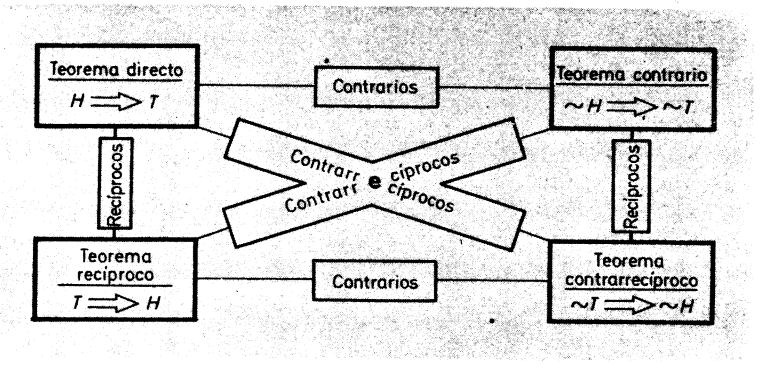
Resulta claro que, establecida una proposición teoremática como directa, tanto la contraria de su recíproca, como la recíproca de su contraria, produce en ambos casos el teorema contrarrecíproco del directo.

Ejemplo

Directo: Si $P(a) = 0$, entonces $P(x) = \overset{\cdot}{\overline{x - a}}$.

Contrarrecíproco: Si $P(x) \neq \overset{\cdot}{\overline{x - a}}$, entonces $P(a) \neq 0$.

A continuación facilitamos un cuadro comparativo de las cuestiones que se vienen estableciendo.



Compréndase que la certeza de una cualquiera de las formas enunciativas de un teorema no implica la certeza de las restantes, excepto la de su contrarrecíproca (consúltese la ley de transposición T_{15} del núm. 1.1333).

Ejemplo

«Si dos ángulos son adyacentes, éstos son suplementarios.»

Este teorema, correcto, no implica la certeza de su recíproco:

«Si dos ángulos son suplementarios, son adyacentes»,

enunciación evidentemente falsa; tampoco la de su contrario:

«Si dos ángulos no son adyacentes, no son suplementarios»,

tan falsa como la anterior.

Sin embargo, la proposición inicial es una proposición equivalente a su contrarrecíproca:

«Si dos ángulos no son suplementarios, no son adyacentes.»

1.155. Condición necesaria y suficiente: proposición *total*

Es muy frecuente en Matemáticas encontrar la locución «la condición necesaria y suficiente para T es H», al enunciar un teorema.

Conviene dejar muy claro que cuando se escribe esto, en realidad, se están enunciando dos teoremas que habrán de ser demostrados ambos, por separado.

Desdoblando la frase, «la condición necesaria para T es H» quiere decir que

$$T \Rightarrow H;$$

«la condición suficiente para T es H» equivale a plantear

$$H \Rightarrow T$$

De modo que estamos frente a un teorema directo, $H \Rightarrow T$, y a su recíproco, $T \Rightarrow H$. El teorema completo quedará demostrado cuando se demuestren el teorema directo y el teorema recíproco*.

Finalmente, y si, en efecto, $H \Rightarrow T$ y $T \Rightarrow H$, nos encontramos frente a la equivalencia lógica

$$H \Leftrightarrow T$$

que indica que la proposición-hipótesis y la proposición-tesis son equivalentes.

Ejemplo

Teorema de Ruffini: La condición necesaria y suficiente para que un polinomio $P(x)$ sea divisible por el binomio $x - a$ es que dicho polinomio se anule, cuando se sustituye la x por la a.

Hipótesis:

$$P(a) = 0$$

Tesis:

$$P(x) = \overset{\cdot}{\overline{x - a}}$$

Teorema:

$$P(a) = 0 \Leftrightarrow P(x) = \overset{\cdot}{\overline{x - a}}$$

Desdoblamiento:

$$\text{Condición necesaria: } P(x) = \overset{\cdot}{\overline{x - a}} \Rightarrow P(a) = 0$$

$$\text{Condición suficiente: } P(a) = 0 \Rightarrow P(x) = \overset{\cdot}{\overline{x - a}}$$

1.16. INDUCCION O RECURRENCIA

Junto al razonamiento deductivo, que hemos venido desarrollando, existen en Matemáticas teoremas, principalmente referentes al conjunto de los números naturales, cuya demostración exige otra técnica de razonamiento, que es la llamada inducción o razonamiento por recurrencia.

---

* Ya que las enunciaciones contrarrecíprocas son lógicamente equivalentes, el mismo resultado *se conseguirá*, si se llegan a demostrar un directo y su contrario.

La inducción matemática está basada en el siguiente

TEOREMA. Sea la función lógica $p(x)$ sobre N. Si $1 \in N_{[1]}$ y $p(n) \Rightarrow p(n+1)$ es cierta, entonces $n \in N_{[1]}$.

Renunciamos a la demostración, pero insistimos en la explicitación de su enunciado.

En términos «menos abstractos» se escribiría:

Si una relación en N se cumple para el natural a, si se consigue probar que, cumpliéndose para x, se cumple para $x+1$, se habrá demostrado que es válida para cualquier natural.

Para demostrar un teorema por inducción hay, pues, que realizar dos fases:

Primera fase: comprobar que la tesis p es cierta para valores concretos de $x \in N$;

Segunda fase: admitido que $p(x)$ es cierta, demostrar que también lo es $p(x+1)$.

Ejemplo

La suma de los n primeros números impares es igual al cuadrado de n.

$$1 + 3 + 5 + \cdots + (2n-1) = n^2 \qquad [1]$$

Primera fase:

para $n = 1$ es cierto que $1 = 1^2$
para $n = 2$ es cierto que $1 + 3 = 2^2$

Segunda fase: Concedamos que la tesis es cierta para $n = m$

$$1 + 3 + 5 + \cdots + (2m-1) = m^2 \qquad [2]$$

Habrá de demostrarse que se cumple para $n = m + 1$.

Veamos:

$$2m + 1 = 2m + 1 \qquad [3]$$

Sumando, miembro a miembro, [2] y [3] resulta:

$$1 + 3 + 5 + \cdots + (2m-1) + (2m+1) = m^2 + 2m + 1$$

$$1 + 3 + 5 + \cdots + (2m-1) + (2m+1) = (m+1)^2 \qquad [4]$$

La igualdad [4] prueba el teorema para $m + 1$.

Así, pues, si $p(1) \in N_{[1]}$ y $p(2) \in N_{[1]}$, $p(2+1)$ también es cierta, y por la misma razón

$$\forall n \in N,\ p(n) \in N_{[1]}$$

1.17. ALGEBRA PROPOSICIONAL

El conjunto de las proposiciones, con las operaciones lógicas de negación ($\sim$), conjunción ($\wedge$) y disyunción ($\vee$), se estructura en *álgebra de Boole*; es decir, se trata de un *retículo complementario distributivo.*

Esta noticia, absolutamente gratuita aquí, pretende dejar la simiente del aprendizaje que, luego, en el capítulo 2.1, se llevará a cabo de una forma consecuente y en profundidad. Allí se hacen constantes referencias a este tema de las proposiciones, y se presentan cuatro posibles sistemas axiomáticos, consistentes entre sí.

Cuando en el número 1.133 se codificaban con una A las seis primeras proposiciones y con una T las restantes, se pretendía ser absolutamente consecuentes con la presentación de la axiomática reticular de las proposiciones, en el ya citado capítulo 2.1: allí se establecerán como axiomas los seis primeros, y los restantes quedan como teoremas, a justificar dentro de ese sistema axiomático.

1.18. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

1.180.

Sea p = «hace calor» y q = «está nublado». Tradúzcanse las siguientes formas proposicionales:

$$\sim p \qquad p \downarrow q$$
$$p \vee q \qquad \sim p \leftrightarrow q$$
$$p \rightarrow \sim q \qquad \sim p \wedge \sim q$$
$$p \veebar q \qquad \sim(\sim p)$$
$$p \barwedge q \qquad (p \vee \sim q) \rightarrow \sim p$$

1.181.

Establézcanse las formas proposicionales de los enunciados siguientes, típicos de un concurso de azafatas:

— Ella es bella y adecuada
— Ella es bella, pero inadecuada
— Ella es fea y adecuada
— Ella ni es fea ni inadecuada
— Si ella es bella, entonces es adecuada
— Si ella es fea o inadecuada, entonces no es adecuada
— Solamente si es ella fea y sólo entonces, ella es inadecuada

1.182.

Determínese el valor de verdad de las siguientes afirmaciones:

$$\text{Si } 4 > 2, \text{ entonces } (4 + i) > (2 + i)$$

(Recuérdese que la relación $>$ no está definida en el conjunto de los complejos.)

$$\text{Si } (4 + i) > (2 + i), \text{ entonces } 4 > 2$$

1.183.

Establézcase la tabla de verdad de las siguientes proposiciones:

$$\sim p \vee q \quad ; \quad (p \wedge q) \rightarrow (p \vee \sim q) \quad ; \quad \sim(p \wedge q) \vee (\sim q \leftrightarrow p)$$

1.184.

Probando que sus bicondicionales son tautológicas, justificar las siguientes equivalencias lógicas:

$$\sim p \Leftrightarrow p \downarrow p \quad ; \quad p \wedge q \Leftrightarrow (p \downarrow p) \downarrow (q \downarrow q) \quad ; \quad p \vee q \Leftrightarrow (p \downarrow q) \downarrow (p \downarrow q)$$

1.185.

Justifíquese la ley condicional de reducción al absurdo (T_{14}).

1.186.

Comprobando que su condicional es tautológica, justifíquese la ley de separación (T_{18}).

1.187.

Sobre el conjunto de definición de los reales, R, se establecen los siguientes enunciados, de los que se piden sus valores de verdad.

$$\forall x \in R,\ |x| = x \qquad \exists x \in R,\ x^2 = x$$
$$\forall x \in R,\ x + 2 > x \qquad \exists^* x \in R,\ |x| = 0$$

1.188.

Encuéntrense contraejemplos que demuestren las siguientes negaciones de proposiciones universales, sobre el conjunto de definición $A = \{2, 3, 4, 5, 6, 7, 8, 9\}$.

$$\sim[\forall x \in A,\ x + 5 < 8] \quad ; \quad \sim[\forall x \in A,\ x^2 > 9]$$
$$\sim[\forall x \in A,\ x = \dot{2}] \quad ; \quad \sim[\forall x \in A,\ 2x < 18]$$

1.189.

Demuéstrese, por inducción, que la suma de los n primeros cubos naturales es igual a

$$\frac{1}{4} \cdot n^2 \cdot (n + 1)^2$$

1.2

Conjuntos

1.21. Introducción

1.22. Términos no definidos: elemento y conjunto

1.23. Relación no definida: pertenencia

1.231. *Descripción*
1.232. *Establecimiento de conjuntos*
1.233. *Representaciones gráficas*
1.234. *Diferencia de conjuntos: el conjunto vacío*

1.24. Inclusión

1.241. *Establecimiento de la relación: subconjuntos*
1.242. *Propiedades de la relación de inclusión*
1.243. *La inclusión de conjuntos y la implicación lógica*
1.244. *Diagramas de inclusión. Comparabilidad*

1.25. Identidad

1.251. *Establecimiento de la relación*
1.252. *Propiedades de la relación de identidad*
1.253. *La identidad de conjuntos y la equivalencia lógica*

1.26. Operaciones conjuntistas

1.261. *Complementación*
1.2611. Conjunto universal
1.2612. Complementación
1.2613. Teorema
1.2614. La complementación de conjuntos y la negación lógica
1.262. *Reunión*
1.2621. Establecimiento de la operación
1.2622. Algunas propiedades de la unión de conjuntos
1.2623. La unión de conjuntos y la disyunción lógica
1.263. *Intersección*
1.2631. Establecimiento de la operación
1.2632. Algunas propiedades de la intersección
1.2633. Conjuntos disjuntos
1.2634. Diferencia simétrica
1.2635. La intersección de conjuntos y la conjunción lógica

1.27. Algebra de las partes de un conjunto. Leyes

1.271. *Conjunto-potencia*
1.272. *Conjuntos finitos y no finitos. Cardinal de un conjunto*
1.273. *Leyes del álgebra de conjuntos*
1.274. *Topología en U. Abiertos y cerrados*
1.2741. Establecimiento
1.2742. Abiertos y cerrados
1.2743. Estructura

1.28. Producto cartesiano

1.281. *Coneepto de pares, ternas, n-tuplas; proyecciones*
1.282. *Definición de producto cartesiano. Representaciones. Generalización*
1.283. *Propiedades*
1.284. *Subconjuntos cartesianos: grafos*

1.29. Aplicabilidad. Automatismos y destrezas

1.2

Conjuntos

1.21. INTRODUCCION

La «teoría de conjuntos» subyace en toda la Matemática, y es la más primaria de todas.

En la base de toda ciencia, enraizada en la filosofía fundamental de la teoría del conocimiento, puede abordarse su estudio desde dos puntos de vista: el intuitivo y el axiomático.

El tratamiento intuitivo de la teoría de conjuntos lleva a contradicciones que destruyen la ciencia; se impone, entonces, el tratamiento axiomático, separado de «evidencias», «sentidos comunes» y «demostraciones físicas».

Sin embargo, fue Georg Cantor, a finales del siglo pasado, quien vino a revolucionar la base de la Matemática, presentando de un modo «ingenuo» (¡fecunda ingenuidad de los sabios!) su teoría de conjuntos, desde un punto de vista intuitivo, no formalizado.

Inmediatamente aparecen las famosas paradojas de Burali-Forti (1897), de Russell, del propio Cantor, entre otras, que, con el fantasma de la contradicción, hacen tambalearse la teoría.

¿Cuál es el error al que la intuición arrastra, y que hace que la teoría de Cantor resulte contradictoria? Tal vez sea la interpretación incorrecta del siguiente teorema*, referible al concepto de subconjunto, determinado por comprensión:

> «Establecido un predicado $p(x)$, para todo conjunto A, existe solamente un subconjunto B, tal que $a \in B$, si y solamente si $a \in A$ y la proposición $p(a)$ es cierta, es decir, $A_{[1]} = B$.»

* Para otros, axioma de especificación.

Demostrado el teorema (y admítase aquí como tal), en contra de lo que pueda dictar la intuición, es falso que para todo predicado $p(x)$ haya un conjunto B, subconjunto de A, que sea su conjunto de validez. El teorema se limita a asegurarlo para un conjunto A, previamente establecido.

Intentemos concretar con un ejemplo:

Sea el predicado sobre A, $a \notin a$. Supongamos que es posible determinar un subconjunto B de A en el que son equivalentes para sus elementos los predicados $a \in A$ y $a \notin a$.

Por el principio de sustitución, se llegaría a establecer la equivalencia contradictoria (!).

$$A \in A \Leftrightarrow A \notin A$$

He aquí la raíz de las paradojas de la teoría de conjuntos.

Con las advertencias que preceden, a las alturas de aprendizaje que se presumen, nosotros intentaremos una exposición conjuntista, en la que un maridaje fecundo entre los dos puntos de vista de su tratamiento ahorrará arideces inútiles, soslayará puntos conflictivos y, al final, abstraerá para crear la estructura booleana del conjunto-potencia.

De este modo se piensa que se acierta en la continuidad que ha de tener todo aprendizaje.

1.22. TERMINOS NO DEFINIDOS: ELEMENTO Y CONJUNTO

Al matematizar la palabra «conjunto», tomado del lenguaje usual, inicialmente se le asigna idéntico significado que el que en su cuarta acepción describe el Diccionario de la Lengua Española:

«**4.** m. Agregado de varias cosas.»

Con esta idea de multiplicidad, el concepto intuitivo «se le queda corto» a la Matemática, que, en seguida, ha de disponer de conjuntos de un solo elemento y de un conjunto con ningún elemento: los conjuntos unitarios y el conjunto vacío, respectivamente.

De todos modos, así advertidos, nosotros arrancamos con el «concepto intuitivo»; y llegado el momento de hacer «retoques matemáticos», se harán explícitamente, para permitir una teoría consistente.

Los objetos que pueden formar un conjunto se denominan elementos.

1.23. RELACION NO DEFINIDA : PERTENENCIA

1.231. Descripción

Uno de los tres signos matemáticos necesarios para desarrollar unas Matemáticas formalizadas, a que aludíamos en 1.11, es el signo de pertenencia, $\in$.

Escribir

$$a \in A$$

es establecer que el elemento a pertenece al conjunto A; mientras que

$$a \notin A$$

significa la negación de la anterior proposición.

1.232. Establecimiento de conjuntos

Un conjunto A se dice que está establecido o que está definido si, dado un objeto a, puede decirse sin ambigüedad que $a \in A$ o que $a \notin A$.

El conjunto de las islas de las Grandes Antillas es un conjunto perfectamente establecido o definido.

Las brujas de Zugarramurdi no definen conjunto, pues, a pesar de las «investigaciones» de Juan Valle Alvarado, Alonso Becerra Holguín y Alonso de Salazar y Frías, de ninguna de las cuarenta inculpadas y llevadas a Logroño, el 8 de junio de 1610, puede asegurarse que fueran o no «bruxas».

Dos son las formas de establecer un conjunto:

a) *Por extensión, tabulación o enumeración*

Se explicitan, entre llaves, todos los elementos.

Ejemplo

El conjunto de componentes minerales del granito

$$A = \{\text{cuarzo, feldespato, mica}\}$$

Aunque parezca la más natural, esta forma de definir un conjunto no siempre es la más útil, y a veces, es inviable. Imagínese la expresión que resultaría, al establecer por extensión, las obras completas del prolífico Lope de Vega que, según Pérez de Montalbán, sobrepasan las cuatrocientas.

Tabular todas las obras del dramaturgo español sería molesto, pero viable; lo que ya no sería factible es establecer por extensión el conjunto de los números naturales, ya que es un conjunto «infinito».

b) *Por comprensión*

Se define un conjunto de esta forma, expresando una proposición cuyo conjunto de validez es precisamente el conjunto a definir.

Para todos los elementos del conjunto, pues, la proposición es cierta y no lo es para cualquier otro objeto que no pertenezca al conjunto.

Ejemplo 1

$$B = \{x/x \text{ es obra escrita por Lope de Vega}\}$$

Ejemplo 2

$$C = \{x/(x \in N) \wedge (x = \dot{2})\}$$

C es el conjunto de todos los x, tales que x es natural y par.

Ejemplo 3

$$D = \{x/(x \in R) \wedge (0 \leq x \leq 1)\}$$

D es el conjunto de todos los números reales comprendidos entre 0 y 1, ambos extremos incluidos.

La proposición p que determina por comprensión a un conjunto X, se la suele denominar «propiedad característica de X».

1.233. Representaciones gráficas

Desde la escuela, los niños están acostumbrados a manejar los diagramas de Venn-Euler, para representar conjuntos.

Ciertamente, son muy útiles y apoyan en la intuición procesos mentales abstractos, no siempre fáciles de seguir; también se muestran muy provechosos para resolver rápidamente problemas con técnica conjuntista. Pero quede claro que nada prueban y que «no son los conjuntos». Como todo ente matemático, el conjunto no es representable. Digamos que es muy útil «representar abstracciones»; pero también muy peligroso, si su fuerza plástica prohíbe o dificulta volver en cualquier momento a la abstracción real del concepto que se maneja.

Ejemplo

$$E = \{x/(x \in Z) \wedge (|x| \leq 2)\}$$

E es el conjunto de todos los enteros cuyo valor absoluto es menor o igual que dos.

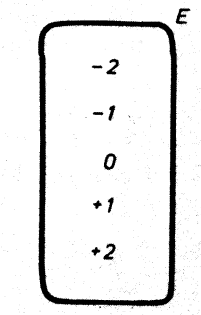


Diagrama de Venn-Euler

Como se ve, se trata de dibujar un recinto plano, cerrado, de forma arbitraria, dentro del cual se disponen los elementos del conjunto que se representa.

1.234. Diferencia de conjuntos: el conjunto vacío

Sean los conjuntos A y B y sean sus propiedades características p y q, respectivamente:

$$A = \{x,\ p(x)\} \quad ; \quad B = \{x,\ q(x)\}$$

Considérese la función lógica compuesta $p(x) \wedge \sim q(x)$, y también la proposición $\forall x,\ p(x) \wedge \sim q(x)$.

El conjunto cuya propiedad característica es la expresada, se denomina *conjunto diferencia*, es decir:

$$A - B = \{x,\ [p(x) \wedge \sim q(x)]\}$$

Todo lo establecido equivale a decir que los elementos del conjunto diferencia son los que, perteneciendo a A, no pertenecen a B, de manera que

$$A - B = \{x/(x \in A) \wedge (x \notin B)\}$$

Inténtese ahora establecer el conjunto diferencia, $A - A$; sus elementos habrían de hacer cierta la proposición contradictoria

$$\forall x,\ p(x) \wedge \sim p(x)$$

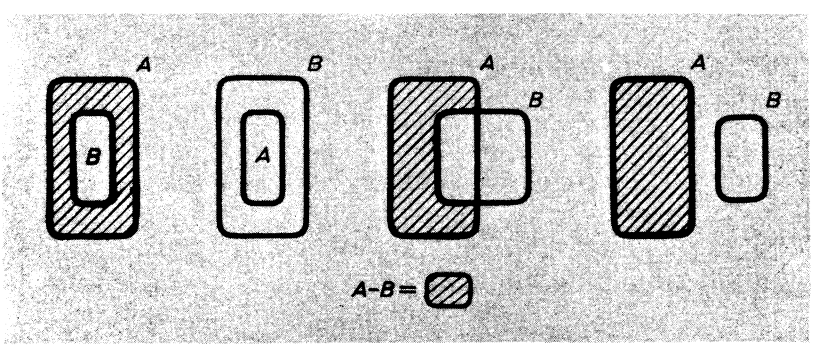
$$A - A = \{x,\ [p(x) \wedge \sim p(x)]\},$$

o bien,

$$A - A = \{x/(x \in A) \wedge (x \notin A)\}$$

Resulta un conjunto «muy especial», pues no existe ningún x que haga cierta una contradicción. Se ha llegado a establecer así, el *conjunto vacío*,

$$\phi = A - A = \{x,\ [p(x) \wedge \sim p(x)]\}$$



Diferencia de conjuntos.

1.24. INCLUSION

1.241. Establecimiento de la relación: subconjuntos

Sean dos conjuntos A y B. Se dice que B está incluido en A o que B es subconjunto de A, y se representa $B \subset A$, si y solamente si todo elemento de B lo es de A; es decir:

$$B \subset A \Leftrightarrow [\forall x \in B \Rightarrow x \in A]$$

Como se desprende de la definición, todo conjunto es subconjunto de sí mismo.

Además, se conviene en admitir que el conjunto vacío es subconjunto de cualquier conjunto.

Resulta entonces que todo conjunto no vacío tiene al menos dos subconjuntos: él mismo y el vacío.

A estos dos subconjuntos se les suele adjetivar en alguna bibliografía de «impropios», para distinguirlos de los otros posibles, que son los «propios». Esos libros, consecuentemente, usan notaciones diferenciadoras: la simbolización $B \subset A$ la reservan para una inclusión «propia»; mientras que escriben $B \subseteq A$ para indicar que B es subconjunto propio o impropio de A.

Ejemplo

Dado $A = \{a, b, c\}$, sus dos subconjuntos impropios y los seis propios son los ocho que se relacionan:

$$\phi,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\}$$

1.242. Propiedades de la relación de inclusión

La relación de inclusión entre conjuntos es reflexiva, antisimétrica y transitiva. En efecto:

Reflexividad:

$$A \subset A$$

Inmediato, de la definición.

Antisimetría:

$$[(B \subset A) \wedge (A \subset B)] \Rightarrow A \equiv B$$

A y B tienen los mismos elementos; son, pues, el mismo conjunto.

Transitividad:

$$[(B \subset A) \wedge (C \subset B)] \Rightarrow (C \subset A)$$

Basta aplicar la ley lógica del mismo nombre, T_{11}.

Como el lector recordará de aprendizajes anteriores, una relación que, como la de inclusión, disfruta de esas tres propiedades, es una relación de orden.

1.243. La inclusión de conjuntos y la implicación lógica

Establezcamos por comprensión el conjunto A y, de igual manera, dando su propiedad característica, un subconjunto propio suyo, B.

— A es el conjunto de todos los x, para los que la proposición p es cierta;
— B es el conjunto de todos los x, para los que la proposición q es cierta.

$$A = \{x,\ p(x)\} \quad ; \quad B = \{x,\ q(x)\}$$
$$B \subset A$$

Si B está incluido en A, es que todo elemento de B cumple la proposición p, que define a A; además, cumplirá su propiedad característica q; de modo que la proposición condicional

$$q(x) \to p(x)$$

resulta ser una tautología, lo que permite establecer la implicación lógica

$$q(x) \Rightarrow p(x).$$

Según se vio en el capítulo anterior, que $q(x)$ implica $p(x)$, quiere decir que

«$q(x)$ es condición suficiente para $p(x)$»

y que

«$p(x)$ es condición necesaria para $q(x)$».

Ejemplo

$$A = \{x/x \text{ es paralelogramo}\}$$
$$B = \{x/x \text{ es rombo}\}$$

Todo rombo es paralelogramo: $B \subset A$
El ser rombo implica ser paralelogramo: $q \Rightarrow p$

— Ser rombo es condición suficiente para ser paralelogramo.
— Ser paralelogramo es condición necesaria para ser rombo.

Se habrá venido observando la gran similitud de tratamiento de la inclusión de conjuntos y la implicación lógica. Ambas juegan el mismo papel, en el álgebra de conjuntos la una, en la de proposiciones la otra. Las dos se encargarán, en su momento, de ordenar sus respectivos conjuntos.

Sucede que son dos concreciones de una misma «realidad matemática».

Avanzado el curso, próximas abstracciones nos darán el siguiente escalón de la matemática: las estructuras. Entonces, ambas relaciones quedarán «fundidas» en un solo concepto: la relación de orden sobre un álgebra booleana.

1.244. Diagramas de inclusión. Comparabilidad

Dados los conjuntos $A = \{x,\ p(x)\}$ y $B = \{x,\ q(x)\}$, puede suceder que

$$[q(x) \Rightarrow p(x)] \downarrow [p(x) \Rightarrow q(x)],$$

en cuyo caso

$$(B \not\subset A) \wedge (A \not\subset B).$$

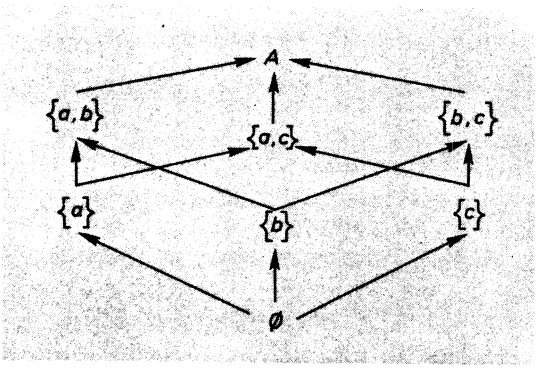
De dos conjuntos, como los establecidos, que no se incluyen, se dice que son «no comparables», siendo «comparables» si

$$(B \subset A) \vee (A \subset B).$$

Una forma cómoda y útil de representar cadenas de inclusiones la constituyen los diagramas lineales. Los ejemplos que siguen son suficientes para su descripción.

Ejemplo 1

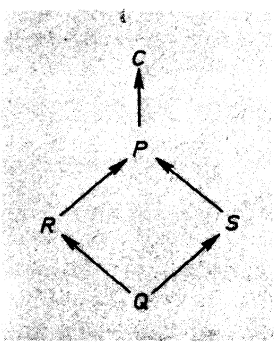
Establecer el diagrama de inclusión de todos los subconjuntos de $A = \{a, b, c\}$.



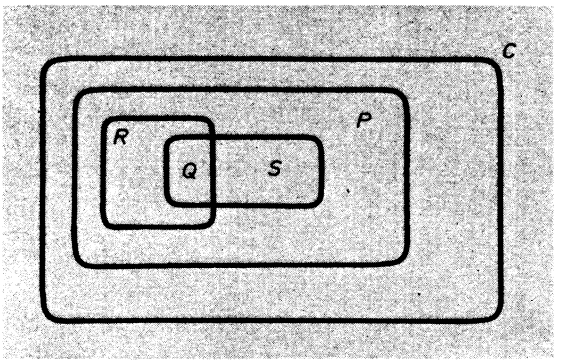
En el ejemplo del núm. 1.241 quedaron establecidos los ocho conjuntos.

Ejemplo 2

Sean $C = \{\text{cuadriláteros}\}$
$P = \{\text{paralelogramos}\}$
$Q = \{\text{cuadrados}\}$
$R = \{\text{rectángulos}\}$
$S = \{\text{rombos}\}$



Sería un buen ejercicio establecer el diagrama de Venn, correspondiente al de inclusión. Analícese que es éste:



Se habrá observado que en los diagramas de inclusión, los conjuntos comparables se encuentran en los nudos de la red, accesibles por los caminos recorridos en el sentido de la inclusión; y los no comparables se encuentran localizados, de manera que no es posible llegar de uno a otro por la red de inclusión.

1.25. IDENTIDAD

1.251. Establecimiento de la relación

Dos conjuntos A y B diremos que son idénticos o iguales*, y escribiremos $A \equiv B$, si y solamente si todo elemento de A lo es de B y todo elemento de B lo es de A. Simbólicamente,

$$(A \equiv B) \Leftrightarrow [\forall x \in A \Rightarrow x \in B) \wedge (\forall x \in B \Rightarrow x \in A)]$$

Observando el segundo miembro de la equivalencia lógica establecida, se ve que cada uno de los términos de la conjunción que la constituye es la condición para que $A \subset B$ y para que $B \subset A$; de modo que también se puede escribir

$$(A \equiv B) \Leftrightarrow [(A \subset B) \wedge (B \subset A)]$$

Ejemplo

$$A = \{\text{carabelas colombinas}\}$$
$$B = \{\text{Santa María, La Niña, La Pinta}\}$$

$$A \equiv B$$

---

* No es nuestro propósito adentrarnos en la difícil y profunda filosofía de la igualdad o/y identidad. Preténdase manejar el signo correctamente; eso, aquí y ahora, basta.

1.252. Propiedades de la relación de identidad

La relación de identidad de conjuntos es reflexiva, simétrica y transitiva. En efecto:

Reflexividad:

$$A \equiv A$$

Inmediato, de la definición

Simetría:

$$(A \equiv B) \Rightarrow (B \equiv A)$$

Por conmutatividad de la conjunción lógica

Transitividad:

$$[(A \equiv B) \wedge (B \equiv C)] \Rightarrow (A \equiv C)$$

Para justificarlo, basta aplicar la ley lógica del mismo nombre, T_{11}.

Por disfrutar de las tres propiedades establecidas, la identidad de conjuntos es una relación de equivalencia, de la que, sin duda, tendrá ya noticia el lector.

1.253. La identidad de conjuntos y la equivalencia lógica

Sean los conjuntos

$$A = \{x,\ p(x)\} \quad ; \quad B = \{x,\ q(x)\}$$

Admitamos que son conjuntos iguales:

$$A \equiv B;$$

entonces, como $B \subset A$, ha de cumplirse que

$$q(x) \Rightarrow p(x);$$

además, el que $A \subset B$, exige que

$$p(x) \Rightarrow q(x).$$

Resulta claro, pues, que las propiedades características de dos conjuntos iguales son lógicamente equivalentes,

$$p(x) \Leftrightarrow q(x);$$

y se puede enunciar que «la condición necesaria y suficiente para $q(x)$ es $p(x)$».

Basándonos en lo que antecede, diremos entonces que, para justificar que dos conjuntos, dados por comprensión, son iguales, habrá de demostrarse que sus

propiedades características son lógicamente equivalentes, para lo cual ha de mostrarse, a su vez, que su bicondicional es tautológica.

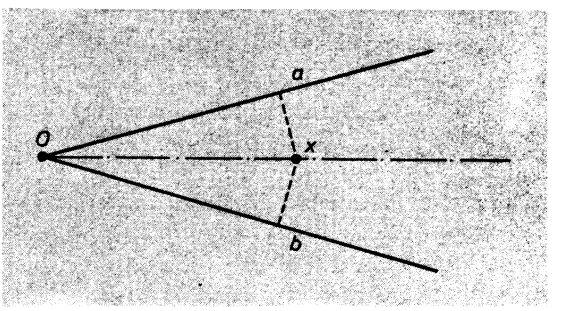
Ejemplo

El método de los «lugares geométricos», tan frecuente en Geometría clásica, no es más que una aplicación de la equivalencia lógica entre las propiedades características de dos conjuntos que se pretenden demostrar iguales. Así, por ejemplo, desarrollamos el siguiente:

> «El lugar geométrico de todos los puntos del plano, equidistantes de dos semirrectas de origen común es la semirrecta-bisectriz del ángulo que forman.»

Los conjuntos que han de demostrarse que son iguales son:

$A = \{x/x$ punto equidistante de a y de $b\}$
$B = \{x/x$ punto de la bisectriz de $\widehat{aOb}\}$



1.º Se justifica que $B \subset A$. Para ello, se prueba que

$q \Rightarrow p$: «si x es un punto de la bisectriz de $\widehat{aOb}$, entonces equidista de a y de b» es tautología.

La Geometría elemental demuestra muy sencillamente que la proposición siempre es cierta.

2.º Se prueba que $A \subset B$, o lo que es igual, se justifica que

$p \Rightarrow q$: «si x equidista de a y de b, entonces x es un punto de la bisectriz de $\widehat{aOb}$» es siempre cierta.

También es simple su justificación geométrica.

3.º Se constata que $p \Leftrightarrow q$, con lo que el lugar geométrico queda establecido, habiendo probado que

$$A \equiv B$$

Una vez definida la complementación de conjuntos, volveremos sobre este ejemplo, a fin de demostrar otra posibilidad de demostración de lugares geométricos.

1.26. OPERACIONES CONJUNTISTAS

Establecidas la relación de igualdad y la relación de orden (inclusión), nos disponemos a crear operaciones entre conjuntos que, en su momento, permitirán estructurar el «conjunto de los conjuntos»*.

1.261. Complementación

1.2611. *Conjunto universal*

Se suele denominar «universal», «conjunto referencia» y también «universo del discurso» al conjunto del que son subconjuntos todos los conjuntos a que se refiere un determinado razonamiento o «discurso».

Así, si se trata de un teorema sobre triángulos en Geometría plana, el conjunto universal es

$$U = \{\text{todos los triángulos planos}\};$$

si se delibera sobre un problema político, a nivel mundial de decisión (?), el conjunto universal debiera ser

$$U = \{\text{O.N.U.}\}$$

1.2612. *Complementación*

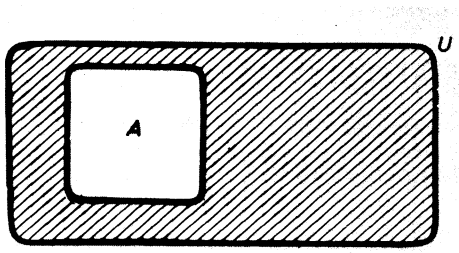
Se denomina así la operación unitaria cuyo resultado es un conjunto formado por todos los elementos del universal, excepto los del conjunto-operando.

Tal definición establece el conjunto complementario de otro como la diferencia entre el universal y el conjunto dado; de modo que se escribe:

$$A' = U - A = \{x/(x \in U) \wedge (x \notin A)\}$$

Ejemplo

Sea el universal $U=\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ y el conjunto $A=\{x/x\in N) \wedge (x=\dot{2})\}$



$$A' = U - A = \{1, 3, 5, 7, 9\}$$

La parte rayada representa A'.

NOTA. El primer término de la conjunción que define a A', en rigor, debiera suprimirse.

---

* Ni con las comillas quedamos tranquilos. Advierta el lector que el «conjunto de los conjuntos» es un concepto paradójico.

En el epígrafe 3.1135 del capítulo 3.1, el teorema de Cantor aclarará la cuestión.

Restricción del concepto. A veces, interesa considerar el complementario de un conjunto A, respecto de otro M, que le incluye, $A \subset M$. El concepto es el mismo, coincide con el de diferencia $M - A$, y la notación debe explicitar claramente el conjunto de referencia; es ésta:

$$A'_M = C_A^M = \{x/(x \in M) \wedge (x \notin A)\}$$

1.2613. TEOREMA. Si $A \subset B$, entonces $B' \subset A'$ y $B - A \equiv A' - B'$.

Demostración

1.º $(A \subset B) \Leftrightarrow (\forall x \in A \Leftrightarrow x \in B)$

$\Downarrow$ según la ley de transposición, T_{15}

$(\forall x \notin B \Rightarrow x \notin A) \Leftrightarrow B' \subset A'$

2.º
$$\begin{aligned} B - A &= \{x/(x \in B) \wedge (x \notin A)\} \\ A' - B' &= \{x/(x \in A') \wedge (x \notin B')\} \\ \forall x \in (B - A) &\Leftrightarrow [(x \in B) \wedge (x \notin A)] \\ &\Updownarrow \text{ por } A_4 \\ &(x \notin A) \wedge (x \in B) \\ &\Updownarrow \\ \forall x \in (A' - B') &\Leftrightarrow (x \in A') \wedge (x \notin B') \end{aligned}$$

1.2614. *La complementación de conjuntos y la negación lógica*

Sean los conjuntos complementarios

$$A = \{x,\ p(x)\} \quad ; \quad A' = \{x,\ q(x)\}$$

Si $[\forall x \in A,\ p(x)]$ es cierta, la proposición $[\forall x \in A',\ p(x)]$ es falsa. Como la proposición de definición $[\forall x \in A',\ q(x)]$ es cierta, resulta que $q(x)$ es la negación de $p(x)$,

$$q(x) \Leftrightarrow \sim p(x),$$

y el conjunto complementario se puede establecer así:

$$A' = \{x,\ \sim p(x)\}$$

Ejemplo

Sea A el conjunto de los naturales primos. Su complementario A' está formado por todos los naturales compuestos (no primos). O sea:

$$\begin{aligned} A &= \{x/x \text{ es natural primo}\} \\ A' = N - A &= \{x/x \text{ es natural no primo}\} \end{aligned}$$

Como venimos insistiendo, la gran similitud de tratamientos entre los términos conjuntistas y proposicionales (aquí, la complementación y la negación) parece

que indica que nos encontramos frente a objetos muy semejantes; pues bien: no se trata de semejanza, lo que ocurre es que son «distintas palabras para las mismas cosas». El ente matemático es único; las descripciones son varias.

Como se prometió en el número anterior, vamos a continuar ahora con el ejemplo de los lugares geométricos.

Quedó dicho que establecer un lugar geométrico se reducía a demostrar la identidad de dos conjuntos, y allí se hizo utilizando la relación

$$(A \equiv B) \Leftrightarrow [(B \subset A) \wedge (A \subset B)],$$

que siendo p y q las propiedades características de A y de B, respectivamente, se reducía a justificar las implicaciones lógicas

$$q \Rightarrow p \quad \text{y} \quad p \Rightarrow q;$$

en fin, que

$$p \Leftrightarrow q$$

Si se consulta el número 1.155, se caerá en la cuenta de que este modo de trabajar es probar una proposición total (un lugar geométrico, por ejemplo), justificando el teorema directo ($H \Rightarrow T$) y su recíproco ($T \Rightarrow H$). Pero allí se apuntaba que otro modo de conseguir la demostración completa es demostrar el teorema directo ($H \Rightarrow T$) y su contrario ($\sim H \Rightarrow \sim T$).

La primera parte del teorema 1.2612, recién demostrado, va a permitir abundar un poco más en el modo de justificar el lugar geométrico, que nos viene sirviendo de ejemplo.

Ahora disponemos de otro modo de demostrar la igualdad de dos conjuntos

$$A \equiv B \Leftrightarrow [(B \subset A) \wedge (A \subset B)] \qquad [1]$$

$$A \equiv B \Leftrightarrow [(B \subset A) \wedge (B' \subset A')] \qquad [2]$$

La forma [2] de abordar la demostración equivale a justificar el directo y el contrario. Veamos:

1.º Se justifica que $B \subset A$, de igual modo que se hizo antes.

2.º Se demuestra que $B' \subset A'$

$\sim q \Rightarrow \sim p$: «si x no es un punto de la bisectriz de $\widehat{aOb}$, entonces no equidista de a y de b», es tautología.

3.º $[(q \Rightarrow q) \wedge (\sim q \Rightarrow \sim p)] \Leftrightarrow (p \Leftrightarrow q)$.

El lugar queda establecido, habiéndose demostrado, de este modo, que

$$A \equiv B$$

1.262. Reunión

1.2621. *Establecimiento de la operación*

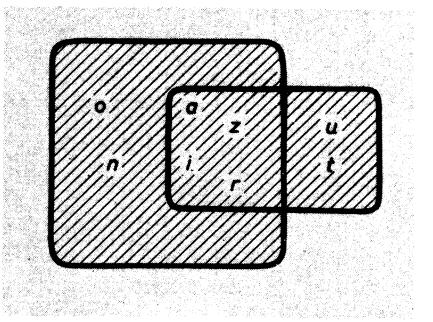
Se llama reunión o unión de dos conjuntos A y B otro conjunto, denotado $(A \cup B)$, formado por los elementos que pertenecen a A o que pertenecen a B o a ambos. Simbólicamente:

$$A \cup B = \{x/(x \in A) \vee (x \in B)\}$$

Ejemplo

$$A = \{a, z, o, r, i, n\}$$
$$B = \{z, u, r, i, t, a\}$$

$A \cup B = \{a, z, o, r, i, n, u, t\}$
(Se ha rayado $A \cup B$.)



1.2622. *Algunas propiedades de la unión de conjuntos**

Siendo A, B y C subconjuntos del universal U, se localizan aquí estas primeras seis propiedades:

A_4) *Conmutatividad*:

$$A \cup B \equiv B \cup A$$

Se postula, siguiendo a Huntington.

T_2) *Idempotencia*:

$$A \cup A \equiv A$$

En efecto:

$$[\forall x \in A \Rightarrow x \in (A \cup A)] \Rightarrow A \subset (A \cup A);$$
$$[\forall x \in (A \cup A) \Rightarrow x \in A] \Rightarrow (A \cup A) \subset A.$$

T_3) *Asociatividad*:

$$A \cup (B \cup C) \equiv (A \cup B) \cup C$$

* Codificamos A o T, según sean axiomas o teoremas, siguiendo el sistema booleano de Huntington. Los subíndices conservan la ordenación del capítulo 1.1 y se corresponden con la relación del 2.1.

Basta para justificarla, probar la inclusión recíproca, como se acaba de hacer en T_2.

$$[x \in A \cup (B \cup C)] \Rightarrow [(x \in A) \vee x \in (B \cup C)] \Rightarrow [(x \in A) \vee (x \in B \vee x \in C)] \Rightarrow$$
$$\Rightarrow [(x \in A \vee x \in B) \vee x \in C] \Rightarrow [x \in (A \cup B) \vee x \in C] \Rightarrow [x \in (A \cup B) \cup C]$$
$$A \cup (B \cup C) \subset (A \cup B) \cup C \qquad [1]$$

y la inclusión recíproca,

$$[x \in (A \cup B) \cup C] \Rightarrow [x \in (A \cup B) \vee x \in C] \Rightarrow [(x \in A \vee x \in B) \vee x \in C] \Rightarrow$$
$$\Rightarrow [x \in A \vee (x \in B \vee x \in C)] \Rightarrow [x \in A \vee x \in (B \cup C)] \Rightarrow [x \in (A \cup (B \cup C))]$$
$$(A \cup B) \cup C \subset A \cup (B \cup C) \qquad [2]$$

Las inclusiones [1] y [2] prueban T_3.

T_{10}) *Simplificación*:

$$A \subset A \cup B \quad ; \quad B \subset A \cup B$$

En efecto:

$$[\forall x \in A \Rightarrow x \in (A \cup B)] \Rightarrow A \subset A \cup B$$
$$[\forall x \in B \Rightarrow x \in (A \cup B)] \Rightarrow B \subset A \cup B$$

T_{14}) *Implicación-reunión*:

$$(A \subset B) \Leftrightarrow [(A' \cup B) \equiv U]$$
$$(A \subset B) \Leftrightarrow [\forall x \in A \Rightarrow x \in B] \Leftrightarrow [\forall x \notin A' \Rightarrow x \in B] \Rightarrow (A' \cup B) \equiv U$$
$$[(A' \cup B) \equiv U] \Rightarrow [\forall x \notin A' \Rightarrow x \in B] \Leftrightarrow [\forall x \in A \Rightarrow x \in B] \Rightarrow A \subset B$$

T_{17}) *Expansión*:

$$(A \cup B \equiv B) \Leftrightarrow A \subset B$$
$$[(A \cup B) \equiv B] \Rightarrow (\forall x \in A \Rightarrow x \in B) \Rightarrow A \subset B$$
$$(A \subset B) \Leftrightarrow (\forall x \in A \Rightarrow x \in B) \Rightarrow (A \cup B \equiv B)$$

1.2623. *La unión de conjuntos y la disyunción lógica*

Sean los conjuntos

$$A = \{x,\ p(x)\} \quad \text{y} \quad B = \{x,\ q(x)\}.$$

Cada elemento de la reunión $(A \cup B)$ cumple la propiedad $p(x)$, si sólo pertenecía a A; la $q(x)$, si procedía exclusivamente de B; y si era un elemento común a ambos conjuntos reunidos, entonces cumple las dos. Así, pues, la proposición

$$[\forall x \in (A \cup B),\ p(x) \vee q(x)]$$

es tautológica; luego la unión de dos conjuntos, establecidos por comprensión, tiene por propiedad característica la disyunción de las proposiciones definitorias de los reunidos:

$$A \cup B = \{x,\ (p(x) \vee q(x))\}$$

Ejemplo

$$A = \{x/x \text{ es animal } ♀\}$$
$$B = \{x/x \text{ es animal } ♂\}$$
$$A \cup B = \{x/x \text{ es animal sexuado}\}$$

Y un equinodermo (erizo de mar), que es hermafrodita (⚥), ¿a qué conjunto pertenece?; ¿al A o al B? Es un elemento común a ambos y como tal, también aparece en la reunión $A \cup B$.

1.263. Intersección

1.2631. *Establecimiento de la operación*

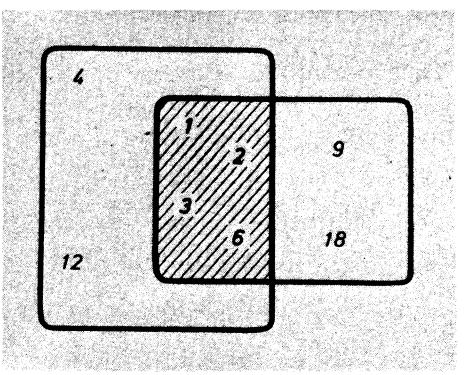
Se llama intersección de dos conjuntos A y B a otro conjunto, denotado $(A \cap B)$, formado por los elementos comunes de los conjuntos intersecados. Simbólicamente:

$$A \cap B = \{x/(x \in A) \wedge (x \in B)\}$$

Ejemplo

$$A = \{x/x \text{ es divisor natural de } 12\} = \{1, 2, 3, 4, 6, 12\}$$
$$B = \{x/x \text{ es divisor natural de } 18\} = \{1, 2, 3, 6, 9, 18\}$$
$$A \cap B = \{x/x \text{ es divisor común de } 12 \text{ y } 18\} = \{1, 2, 3, 6\}$$

(Se ha rayado $A \cap B$)



1.2632. *Algunas propiedades de la intersección de conjuntos*

A_4) *Conmutatividad*:

$$A \cap B \equiv B \cap A$$

Se postula, siguiendo a Huntington.

T_2) *Idempotencia*:

$$A \cap A \equiv A$$

T_3) *Asociatividad*:

$$A \cap (B \cap C) = (A \cap B) \cap C$$

T_{10}) *Simplificación*:

$$A \cap B \subset A \quad ; \quad A \cap B \subset B$$

T_{17}) *Expansión*:

$$(A \cap B \equiv A) \Leftrightarrow (A \subset B)$$

Las demostraciones de las leyes T enunciadas son del todo similares a las realizadas para la reunión. Se dejan para ejercicio del lector.

1.2633. *Conjuntos disjuntos*

Se denominan así dos conjuntos que no tienen elementos comunes. Consecuentemente, su intersección es el conjunto vacío. Se define:

$$\left.\begin{array}{l} A \text{ y } B \text{ son conjuntos disjuntos} \end{array}\right\} \Leftrightarrow A \cap B = \phi$$

NOTA. En algunos libros, cuando se trata de la unión de dos conjuntos disjuntos, es frecuente encontrar una denominación específica: adición de conjuntos. Se denota como se indica en la definición:

$$(A + B = C) \Leftrightarrow [(A \cap B = \phi) \wedge (A \cup B = C)]$$

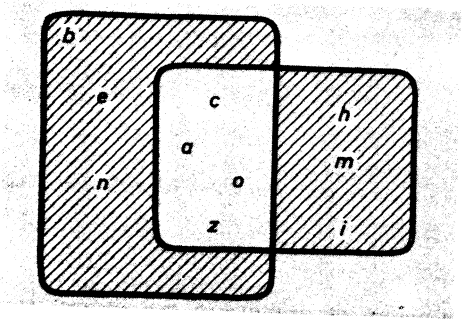
1.2634. *Diferencia simétrica*

Recibe este nombre la operación que se simboliza

$$A \triangle B \equiv (A \cup B) - (A \cap B)$$

Ejemplo

$$A = \{c, a, b, e, z, o, n\}$$
$$B = \{c, h, a, m, i, z, o\}$$
$$A \triangle B = \{b, e, n, h, i, m\}$$



(En el esquema se ha rayado $A \triangle B$.)

La operación lógica que se corresponde con esta diferencia simétrica de conjuntos es la disyunción exclusiva ($\underline{\vee}$) y, efectivamente, el establecimiento por comprensión de la diferencia simétrica así lo pone de manifiesto:

$$A = \{x,\ p(x)\} \quad ; \quad B = \{x,\ q(x)\}$$
$$A \triangle B = \{x,\ p(x) \mathbin{\underline{\vee}} q(x)\}$$

TEOREMA. La diferencia simétrica también se puede establecer de este modo:

$$A \triangle B \equiv (A - B) \cup (B - A)$$

En efecto:

$$[\forall x \in (A \triangle B)] \Rightarrow [(x \in A) \vee (x \in B) \wedge x \notin (A \cap B)] \Rightarrow$$
$$\Rightarrow [(x \in A) \wedge (x \notin B)] \vee [(x \in B) \wedge (x \notin A)] \Rightarrow x \in [(A - B) \cup (B - A)]$$
$$A \triangle B \subset [(A - B) \cup (B - A)] \qquad [1]$$
$$[\forall x \in [(A - B) \cup (B - A)]] \Rightarrow [x \in (A - B) \vee x \in (B - A)] \Rightarrow$$
$$\Rightarrow [(x \in A) \wedge (x \notin B) \vee (x \in B) \wedge (x \notin A)] \Rightarrow [x \in (A \cup B) \wedge x \notin (A \cap B)]$$
$$[(A - B) \cup (B - A)] \subset A \triangle B \qquad [2]$$

Las inclusiones [1] y [2] justifican la identidad del teorema.

1.2635. *La intersección de conjuntos y la conjunción lógica*

Sean dos conjuntos $A = \{x,\ p(x)\}$ y $B = \{x,\ q(x)\}$, establecidos mediante sus propiedades características.

Cada elemento de la intersección $A \cap B$ ha de cumplir el predicado $p(x)$ y también el $q(x)$, ya que es común a ambos conjuntos. Entonces, la proposición

$$[\forall x \in (A \cap B),\ p(x) \wedge q(x)]$$

es una tautología; luego la intersección de dos conjuntos tiene por propiedad característica la conjunción de las propiedades definitorias de los conjuntos intersecados:

$$A \cap B = \{x,\ p(x) \wedge q(x)\}$$

1.27. ALGEBRA DE LAS PARTES DE UN CONJUNTO. LEYES

1.271. Conjunto-potencia

Sea el universal U. Denotamos por $P(U)$ el conjunto de todos sus subconjuntos, incluidos —por supuesto— el ϕ y el propio U.

A $P(U)$ se le denomina conjunto de las partes de U y también conjunto-potencia.

Obsérvese que los elementos del conjunto-potencia $P(U)$ son, a su vez, conjuntos

Ejemplo

$$U = \{a, b, c\}$$
$$P(U) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, U\}$$

1.272. Conjuntos finitos y no finitos. Cardinal de un conjunto

Entiéndase que los establecimientos «intuitivos» que siguen son del todo insuficientes y que, de aferrarse a ellos hasta sus últimas consecuencias, conducirían irremediablemente a paradojas o contradicciones, sin salida posible.

Sin embargo es útil disponer ya de estos conceptos; y aun cuando todavía no se haya construido la teoría de la numerabilidad, que permitiría su establecimiento correcto, con la advertencia que precede, se escribe de un modo simplista: Conjunto finito es el que tiene un número «determinado» de elementos; conjunto no finito es el que tiene un «número infinito» de elementos.

Ejemplo

Conjuntos finitos

$A = \{\text{átomos de un átomo gramo}\}$
$B = \{x/x \text{ es as de la baraja española}\}$
$C = \{x/x \text{ es hijo de Carlos II el Hechizado}\}$

Conjuntos no finitos

$N = \{\text{números naturales}\}$
$D = \{\text{números naturales pares}\}$
$Z = \{\text{números enteros}\}$
$E = \{\text{números primos}\}$
$Q = \{\text{números racionales}\}$
$F = \{x/(x \in Q) \wedge (0 < x < 1)\}$

Se llama cardinal o potencia de un conjunto A, y se denota $\text{card}(A)$ y también $n(A)$, al número de sus elementos.

Así, los cardinales de los ejemplos anteriores son:

$$\text{card}(A) = 6{,}06 \times 10^{23},$$

pues, según Avogadro, ése es el número de átomos que hay en un átomo gramo de cualquier sustancia.

$$\text{card}(B) = 4,$$

como es del dominio público.

$$\text{card}(C) = 0$$

La Historia asegura que Carlos II no tuvo hijos, de modo que $\text{card}(\phi) = 0$.

Los restantes conjuntos no finitos habremos de decir aquí que sus cardinales o potencias es «infinito».

Sin embargo, obsérvese de paso, que, por ejemplo, N tiene infinitos elementos y D también, lo cual no importa para que, evidentemente, $D \subset N$.

Lo mismo sucede con E y Z, e igual con F y Q.

¿Habrá distintos «infinitos»? Sugerente pregunta (aunque muy incorrectamente expresada) que será debidamente contestada en su momento.

Cardinal del conjunto-potencia

Si U es un conjunto finito, se demuestra en Combinatoria* que el cardinal del conjunto de sus partes es

$$\text{card}[P(U)] = 2^n,$$

siendo n el número de elementos de U.

Ejemplo

$$\text{Sea } U = \{x, y, z\}$$

$$\text{card}[P(U)] = 2^3 = 8$$

1.273. Leyes del álgebra de conjuntos

Sea el referencial o universal U, y sobre el conjunto de sus partes, $P(U)$, las operaciones complementación ($'$), unión ($\cup$) e intersección ($\cap$), que han sido

---

* Sea A un conjunto finito y $\text{card}(A) = n$. El conjunto de sus partes, $P(A)$, está formado por: el conjunto vacío, que se contabiliza $1 = \binom{n}{0}$; los n conjuntos unitarios, que son las combinaciones unitarias de sus n elementos: $\binom{n}{1}$; los conjuntos binarios, que son las combinaciones binarias de sus n elementos: $\binom{n}{2}$; y de este modo, ha de contabilizarse hasta el propio A, que con sus n elementos, es la única combinación n-aria: $\binom{n}{n}$. Así, el número de elementos de $P(A)$ es:

$$\text{card } P(A) = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n};$$

de otro lado, según Newton,

$$2^n = (1+1)^n = \binom{n}{0} 1^n \cdot 1^0 + \binom{n}{1} 1^{n-1} \cdot 1^1 + \cdots + \binom{n}{n} 1^0 \cdot 1^n.$$

Resultando la misma expresión, es, pues

$$\text{card}[P(A)] = 2^n.$$

establecidas. La cuaterna $[P(U), ', \cup, \cap]$ obedece, entre otras, a las siguientes *:

T_1) *Absorción*

$$A \cup (A \cap B) = A \quad ; \quad A \cap (A \cup B) = A$$

Se justifica la primera. Análoga demostración establece la segunda.

$$[\forall x \in [A \cup (A \cap B)] \Rightarrow [(x \in A) \vee (x \in A \wedge x \in B)] \Rightarrow$$
$$\Rightarrow [(x \in A) \wedge (x \in A \vee x \in B)] \Rightarrow$$
$$\Rightarrow x \in A \quad ; \quad \underline{A \cup (A \cap B) \subset A}$$
$$[\forall x \in A] \Rightarrow [(x \in A) \wedge (x \in A \vee x \in B)] \Rightarrow [(x \in A) \vee (x \in A \wedge x \in B)] \Rightarrow$$
$$\Rightarrow x \in A \cup (A \cap B); \quad \underline{A \subset A \cup (A \cap B)}$$

T_2) *Idempotencia*

$$A \cup A = A \quad ; \quad A \cap A = A$$

Quedó justificada anteriormente.

T_3) *Asociatividad*

$$A \cup (B \cup C) = (A \cup B) \cup C \quad ; \quad A \cap (B \cap C) = (A \cap B) \cap C$$

Se ha demostrado anteriormente.

A_4) *Conmutatividad*

$$A \cup B = B \cup A \quad ; \quad A \cap B = B \cap A$$

A_5) *Complementariedad*

$$A \cup A' = U \quad ; \quad A \cap A' = \phi$$

A_6) *Distributividad*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad ; \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

A_7) *Identidad*

$$A \cup \phi = A \quad ; \quad A \cap U = A$$

---

* En proposiciones, «preparando» la axiomática reticular, se codificaban con A (= axioma) las seis primeras leyes. Aquí podíamos hacer lo mismo; pero también, para «preparar» el importante capítulo 2.1, en el que al desarrollar en abstracto el álgebra de Boole, se cosechará el rendimiento de estos aprendizajes previos, codificamos con A de la cuarta a la séptima, ambas inclusive, que constituyen el sistema axiomático de Huntington, equivalente al reticular.

Por lo demás, no se desazone el lector por estas cuestiones —por ahora—, ya que, como queda dicho, el capítulo 2.1 le dará la panorámica completa de estos aprendizajes, que se han presentado absolutamente conexos.

T_8) *Involución*

$$(A')' = A$$

Sea $B \in P(U)$;

Por complementariedad (A_5):

$$B \cup B' = U \quad ; \quad B \cap B' = \phi \qquad [1]$$

Por conmutatividad (A_4):

$$B' \cup B = U \quad ; \quad B' \cap B = \phi \qquad [2]$$

Supóngase que $B' \equiv A$; entonces, en [2],

$$(A')' \cup A' = U \quad ; \quad (A')' \cap A' = \phi \qquad [3]$$

Como el axioma de complementariedad (A_5) ha de cumplirse, sucede que

$$A \cup A' = U \quad ; \quad A \cap A' = \phi \qquad [4]$$

y, si el complementario es único*, al comparar las expresiones [3] y [4] resulta necesariamente que

$$(A')' = A$$

Consecuencia inmediata del teorema es el corolario

t_8) $$(\phi' \equiv U) \wedge (U' \equiv \phi)$$

T_9) *Ley de De Morgan*

$$(A \cup B)' = A' \cap B' \quad ; \quad (A \cap B)' = A' \cup B'$$

$$[\forall x \in (A \cup B)'] \Rightarrow x \notin (A \cup B) \Rightarrow [(x \notin A) \wedge (x \notin B)] \Rightarrow$$
$$\Rightarrow [(x \in A') \wedge (x \in B')] \Rightarrow x \in (A' \cap B');$$
$$(A \cup B)' \subset A' \cap B' \qquad [5]$$

recíprocamente:

$$[\forall x \in (A' \cap B') \Rightarrow [(x \in A') \wedge (x \in B')] \Rightarrow [(x \notin A) \wedge (x \notin B)] \Rightarrow$$
$$\Rightarrow [x \notin (A \cup B)] \Rightarrow [x \in (A \cup B)'];$$
$$A' \cap B' \subset (A \cup B)' \qquad [6]$$

* Una demostración completamente generalizada de este teorema ya se puede consultar en el teorema 5, de la página 117. No procede, pues, su repetición.

De [5] y de [6] se sigue la primera ley de De Morgan. Debe intentarse, como ejercicio, la justificación de la segunda.

T_{10}) En $[P(U), ', \cup, \cap]$ la relación $\subset$ es de orden.

En el número 1.242 ya quedó establecida una, más que demostración, descripción de este punto. Para una rigurosa y general justificación de este T_{10}, aguárdese a llegar al teorema 8, de la página 119.

T_{11}) El orden $[P(U), \subset]$ tiene extremos absolutos, $\cup$ y ϕ.
$\forall A \in P(U)$,

$$\begin{aligned} A \cap \phi &= \phi \cup (A \cap \phi), \text{ según } A_7 \text{ y } A_4; \\ &= (A \cap A') \cup (A \cap \phi), \text{ según } A_5; \\ &= A \cap (A' \cup \phi), \text{ según } A_6; \\ &= A \cap A', \text{ en virtud de } A_7; \\ &= \phi, \text{ en razón de } A_5. \end{aligned}$$

De modo que $\phi = A \cap \phi$

$$\phi = \phi \cap A, \text{ según } A_4$$

$$\Updownarrow$$

$$\phi \subset A$$

Por otra parte, $A = A \cap U \Rightarrow A \subset U$.

T_{12}) *Ley de Dedekind* $A \subset B \Rightarrow A \cup (C \cap B) \equiv (A \cup C) \cap B$

$$A \cup (C \cap B) \equiv (A \cup C) \cap (A \cup B), \text{ según } A_6 \qquad [7]$$

$$A \subset B \Rightarrow (A \cup B) = B \qquad [8]$$

sustituyendo [8] en [7],

$$A \cup (C \cap B) \equiv (A \cup C) \cap B$$

1.274. Topología en U. Abiertos y cerrados

1.2741. *Establecimiento*

Sea el universal U y $P(U)$ el conjunto de sus partes. Considérese un subconjunto de $P(U)$, T, tal que:

1.º Los subconjuntos impropios, ϕ y U, pertenecen a T;
2.º la unión en T es una operación cerrada; o sea, que la unión de un número cualquiera de conjuntos de T produce un conjunto de T;
3.º la intersección finita en T es una operación cerrada; a saber, que al intersecar entre sí cualquier número finito de conjuntos de T, el resultado es un conjunto de T.

A un $T \subset P(U)$, con las características descritas, se le denomina una topología *en U*. Simbólicamente:

$$\left.\begin{array}{l} T \subset P(U), \text{ es topología en } U \end{array}\right\} \Leftrightarrow (\phi \in T) \wedge (U \in T) \wedge [\forall A \in T \Rightarrow (\bigcup_i A \in T) \wedge (\bigcap_i A \in T)]$$

1.2742. *Abiertos y cerrados*

Se denomina *abierto* a todo conjunto que pertenece a T; y *cerrado* a cada uno de los complementarios de los abiertos. De modo que

$$\left.\begin{array}{l} A \text{ es abierto} \\ \text{de } T \end{array}\right\} \Leftrightarrow A \in T \quad ; \quad \left.\begin{array}{l} A \text{ es cerrado} \\ \text{de } T \end{array}\right\} \Leftrightarrow A' \in T$$

1.2743. *Estructura*

Los abiertos de una topología T forman un *retículo distributivo*, por cumplir las leyes:

T_1) Absorción
T_2) Idempotencia
T_3) Asociatividad
A_4) Conmutatividad
A_6) Distributividad

Cuando se alcance el estudio del capítulo 2.1, bueno será volver sobre este punto, para entender lo escrito y constatar que una topología no llega a ser un álgebra de Boole por no cumplir la ley de complementariedad (A_5).

1.28. PRODUCTO CARTESIANO

1.281. Concepto de pares, ternas, n-tuplas; proyecciones

Sean a y b dos objetos matemáticos preestablecidos, y en ese orden. Se crea una nueva abreviatura matemática (una de las tres fundamentales de las matemáticas «formalizadas»), denominada *par* y denotada (a, b), que ha de obedecer al siguiente criterio axiomático de igualdad:

«Los pares (a, b) y (c, d) son iguales si, y solamente si, $a = c$ y $b = d$.»

Simbólicamente:

$$(a, b) \equiv (c, d) \Leftrightarrow (a = c) \wedge (b = d)$$

Adviértase que con dos objetos matemáticos distintos, a y b, es posible formar dos pares diferentes: el (a, b) y el (b, a).

Permítase el lector descender a la génesis de la abstracción matemática: la vida.

Sea a el código de una blusa, dentro del conjunto de ellas, de una colección ibicenca; y digamos que b representa una determinada pieza de la colección de pantalones, que presenta la misma casa de modas de la isla.

Si la encantadora turista Fanny ha decidido adquirir la blusa a y el pantalón b, diremos que ha adquirido el conjunto (¡cuidado!, no matemático) de piezas (a, b); y no el (b, a), pues aun hoy, tal vez resultara estrambótico, todavía, utilizar ambas prendas, dislocadas de sus topías tradicionales.

Entiéndase que con el ejemplo se pretende aclarar lo esencial del orden en el establecimiento de un par: decir a, es decir una blusa (por ser la primera cita); escribir b es referirse a un pantalón (indicando que es el segundo objeto). En fin

$$(a, b) \not\equiv (b, a)$$

Nada más sencillo que generalizar el concepto de *par* a un número mayor de objetos constituyentes de la abreviatura; así se crean las *ternas* (a, b, c), y en general, las llamadas *n-tuplas*, constituidas por n objetos establecidos en un determinado orden, que es su esencia.

Constituido el par (a, b), se denomina *primera proyección* del par a su primer objeto, siendo la *segunda proyección* el objeto dado en segundo lugar:

$$\mathrm{pr}_1(a, b) \equiv a \quad ; \quad \mathrm{pr}_2(a, b) \equiv b$$

1.282. Definición de producto cartesiano. Representaciones. Generalización

Sean los conjuntos A y B. Se denomina producto cartesiano de A por B, y en este orden, al conjunto de todos los pares que puedan formarse, con primera proyección, perteneciente a A y con segunda proyección, perteneciente a B. Simbólicamente:

$$A \times B = \{(a, b)/(a \in A) \wedge (b \in B)\}$$

Ejemplo 1

Sea A el conjunto de coches de un magnate:

$$A = \{\text{Rolls, Mercedes, Lancia, Ford, Seat}\}$$

y sea B el conjunto de sus «pañuelos de cuello»:

$$B = \{\text{lunares, azul, blanco, negro}\}$$

El producto cartesiano $A \times B$ está formado por todas las posibles combinaciones que puede hacer, conduciendo uno de sus coches, portando uno de sus pañuelos. Si se utilizan iniciales,

$$A \times B = \{(R, 1), (R, a), (R, b), (R, n), (M, 1), (M, a), \ldots, (S, n)\}$$

El número de pares posibles es $5 \times 4 = 20$, de modo que $\mathrm{card}(A \times B) = 20$.

Ejemplo 2

El indio Basha tiene cinco hijos, y en su exigua despensa dispone de cuatro cosas: una escudilla de arroz, un racimo de dátiles, una arenque y un bote de frijoles.

Si es H el conjunto de los hijos de Basha y V el de viandas de que dispone, el producto cartesiano $H \times V$ es el conjunto de todos los pares posibles niño-comida.

Idéntico al ejemplo primero, son 20, también aquí, los pares:

$$\text{card}(H \times V) = 20$$

Naturalmente que es posible extender el concepto al producto cartesiano de un conjunto por sí mismo, en cuyo caso es frecuente utilizar la notación potencial

$$A \times A = A^2$$

Ejemplo

Establézcanse todos los posibles diptongos y replicaciones vocales del idioma español.

Sea V el conjunto de las vocales:

$$V = \{a,\ e,\ i,\ o,\ u\}$$

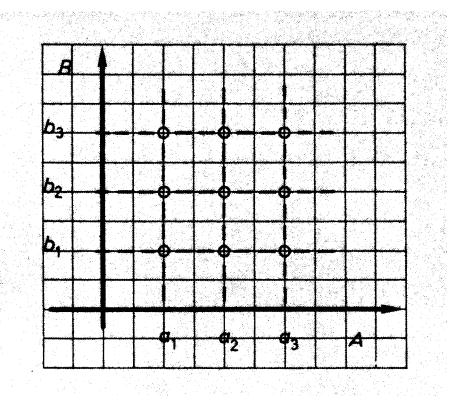
Queda resuelta la cuestión, planteando el producto cartesiano $V \times V$:

$$V \times V = \{(a, a),\ (a, e),\ (a, i),\ \ldots,\ (u, u)\}$$
$$\text{card}(V^2) = 5 \times 5 = 5^2 = 25$$

Representación gráfica

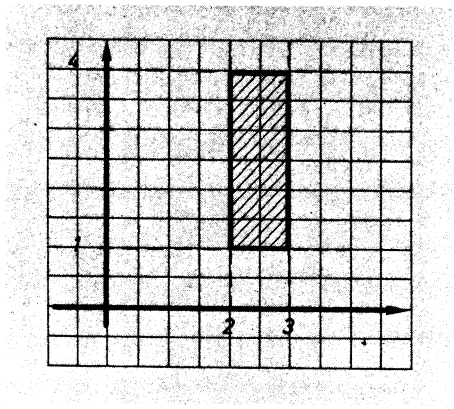
Sean el conjunto $A = \{a_1, a_2, a_3\}$ y el $B = \{b_1, b_2, b_3\}$. Se establece su producto cartesiano, $A \times B$.

Para representar cada uno de los pares de $A \times B$, se traza un sistema ortogonal de ejes. Sobre el horizontal, se registran los elementos de A, y sobre el vertical, los de B, de modo que cada uno de los nudos de la red que resulta, al trazar por las marcas de registro, paralelas a los ejes, representa cada uno de los pares del producto $A \times B$.



Considérense ahora dos conjuntos infinitos, tales son los cerrados* [2, 3] y [1, 4] del conjunto de los reales.

Al representar su producto cartesiano sobre unos ejes ortogonales, no es posible registrar «marcas» en cada eje, representativas de los elementos de los conjuntos operados: son infinitos los elementos de los cerrados, como infinitos son los puntos de los segmentos que los representan.



Sin embargo, sí puede quedar representado el producto cartesiano [2, 3] × [1, 4], no por nudos de la red —como antes—, sino por los infinitos puntos del rectángulo que se raya en la figura, incluidos sus lados (bordes).

Generalización del producto cartesiano

De un modo análogo a lo que se ha establecido para dos conjuntos, se establece para n, de este modo:

$$A \times B \times C \times \ldots (n = \{(a, b, c, \ldots)/(a \in A) \wedge (b \in B) \wedge (c \in C) \wedge \ldots\},$$

que se lee: «el producto cartesiano de n conjuntos es el conjunto de todas las n-tuplas que se pueden formar, tales que cada uno de los objetos de las tuplas pertenece a cada uno de los conjuntos factores».

Si se trata de un solo factor repetido, la notación potencial también se usa en este caso:

$$A \times A \times A \times \cdots (n = A^n$$

Ejemplo

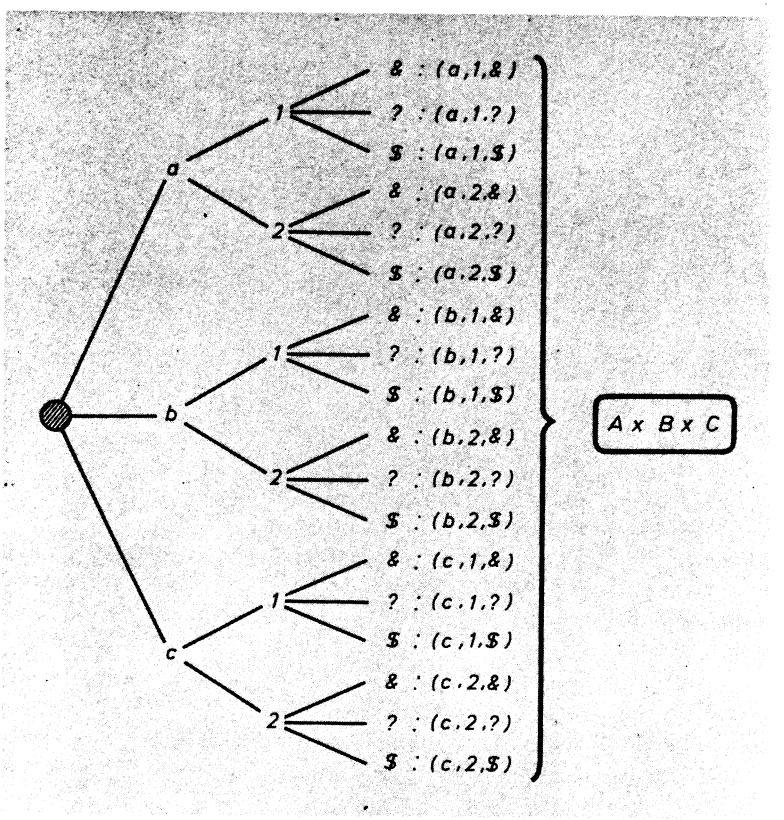
Siendo $A = \{a, b, c\}$, $B = \{1, 2\}$ y $C = \{\&, ?, \$\}$, formar el cartesiano $A \times B \times C$.

---

* Diremos aquí que *cerrados* son subconjuntos de la recta real, que incluyen sus extremos. Así, pues, el cerrado [2, 3] es el segmento de extremos 2 y 3, continente de los infinitos puntos reales de su intervalo.

No es mala técnica para esto utilizar los llamados «diagramas de árbol»; son tan engorrosos como seguros.

La atenta observación por parte del lector, del que se realiza, nos libera de cualquiera otra descripción



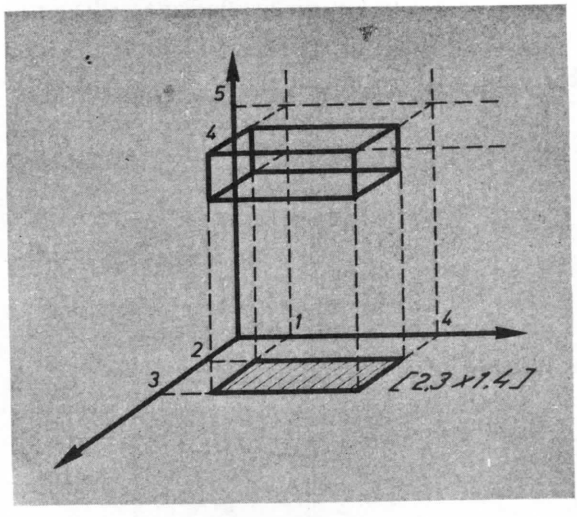
Ejercicio. Demuéstrese que si A y B son dos conjuntos finitos, de potencias respectivas m y n, su producto cartesiano tiene de cardinal $m \times n$.

La representación ortogonal de un producto triple queda sugerida muy fácilmente a partir de la representación que se hizo para el producto cartesiano ordinario de dos conjuntos.

Sean, como antes, los cerrados reales [2, 3], [1, 4] y [4, 5].

Dibujados tres ejes ortoédricos, sobre los de la base se dibuja el rectángulo rayado, que representa el cartesiano binario [2, 3] × [1, 4].

En el eje vertical se registran los extremos del tercer cerrado-factor, que determina en «el espacio», el paralelepípedo que representa el cartesiano triple.



1.283. Propiedades

I. $(A \times B = \phi) \Leftrightarrow (A = \phi \vee B = \phi)$.
(Justifíquese.)

II. $(A \times B \neq \phi) \vee (A = B) \Rightarrow A \times B \neq B \times A$.
(Interprétese y póngase un ejemplo.)

III. $(A \times B) \times C = A \times (B \times C)$*.
En efecto:

$$(A \times B) \times C = \{[(x, y), z]/(x, y) \in A \times B \wedge z \in C\};$$

pero el que $(x, y) \in A \times B$ es equivalente a establecer que $(x \in A) \wedge (y \in B)$, de modo que, introduciendo esta condición en el establecimiento de $(A \times B) \times C$, resulta:

$$(A \times B) \times C = \{[(x, y), z]/(x \in A) \wedge (y \in B) \wedge (z \in C)\}.$$

De otro lado.

$$A \times (B \times C) = \{[x, (y, z)]/(x \in A) \wedge (y, z) \in B \times C;$$

de la misma manera que antes,

$$(y, z) \in B \times C \Leftrightarrow (y \in B) \wedge (z \in C),$$

así es que

---

* En rigor, tal igualdad no es correcta, puesto que las proyecciones de ambos cartesianos son de distinta naturaleza.

$$A \times (B \times C) = \{[x, (y, z)]/(x \in A) \wedge (y \in B) \wedge (z \in C),$$

con lo que queda justificada la asociatividad, establecida en III.

IV. $A \times (B \cup C) = (A \times B) \cup (A \times C) \quad ; \quad A \times (B \cap C) = (A \times B) \cap (A \times C)$

Demostraremos la distributividad respecto de la reunión y dejaremos al lector que justifique, como ejercicio, la distributividad respecto de la intersección.

$$[\forall (x, y) \in A \times (B \cup C)] \Rightarrow (x \in A) \wedge (y \in (B \cup C)) \Rightarrow (x \in A) \wedge [(y \in B) \vee (y \in C)] \Rightarrow$$
$$\Rightarrow [(x \in A) \wedge (y \in B)] \vee [(x \in A) \wedge (y \in C)] \Rightarrow$$
$$\Rightarrow [(x, y) \in A \times B \vee (x, y) \in A \times C] \Rightarrow (x, y) \in (A \times B) \cup (A \times C);$$

luego

$$A \times (B \cup C) \subset (A \times B) \cup (A \times C) \qquad [1]$$

recíprocamente:

$$[\forall (x, y) \in (A \times B) \cup (A \times C)] \Rightarrow (x, y) \in (A \times B) \vee (x, y) \in (A \times C) \Rightarrow$$
$$\Rightarrow [(x \in A) \wedge (y \in B)] \vee [(x \in A) \wedge (y \in C)] \Rightarrow$$
$$\Rightarrow (x \in A) \wedge [(y \in B) \vee (y \in C)] \Leftrightarrow (x \in A) \wedge y \in (B \cup C) \Rightarrow (x, y) \in A \times (B \cup C),$$

lo que demuestra que

$$(A \times B) \cup (A \times C) \subset A \times (B \cup C) \qquad [2]$$

Las inclusiones [1] y [2] justifican IV.

1.284. Subconjuntos cartesianos: grafos

Establecido un cartesiano $A \times B$, se denomina *grafo* a cualquier subconjunto suyo, que denotamos G.

$$G \subset A \times B$$

Según la definición, un grafo es siempre un conjunto de pares, y las denominaciones específicas de éstos se mantienen en él, de modo que a los primeros objetos de sus pares se les sigue llamando primeras proyecciones, y a las segundas se las denomina segundas proyecciones del grafo.

Este concepto alcanzará su máxima utilización al hablar, en el próximo capítulo, de relaciones.

Ejemplo

Sea el cartesiano que se representa por la siguiente matriz

10	1,10	2,10	3,10	4,10
8	1,8	2,8	3,8	4,8
6	1,6	2,6	3,6	4,6
2	1,2	2,2	3,2	4,2
B / A	1	2	3	4

Si del conjunto de pares de $A \times B$ se escogen los sombreados, se obtiene un $G \subset A \times B$,

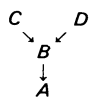
$$G = \{(1, 2),\ (3, 6),\ (4, 8)\},$$

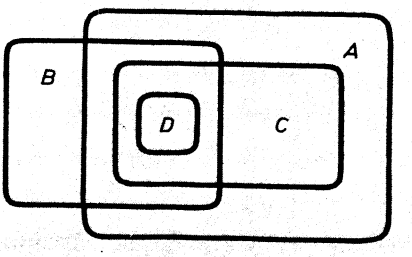
en el que —obsérvense— sus segundas proyecciones son el doble de las primeras. He aquí un primer ejemplo explicitado de relación: «ser doble de».

1.29. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

1.290.

Dibújense todos los posibles diagramas de Venn, correspondientes al de inclusión que se construye. De igual modo, constrúyase el diagrama de inclusión del de Venn que se dibuja.





1.291.

Realícense las siguientes cuestiones:

a) Describir las analogías y diferencias de estos tres conjuntos:

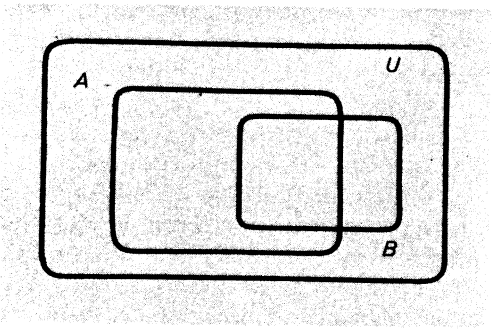
$$\{0\},\ \phi,\ \{\phi\}$$

b) Sobre el conjunto $A = \{a, b, \{c, d\}\}$ se establecen los siguientes predicados: $\{c, d\} \in A$; $\{c, d\} \subset A$; $\{\{c, d\}\} \subset A$; $\{c, d\} \in P(A)$; analícese la corrección o incorrección de cada uno de ellos.

c) Establecer el cardinal del conjunto potencia del conjunto anterior, A.
d) Los conjuntos M y N son no comparables. Constrúyase un diagrama de inclusión de M, N, $(M - N)$, $(N - M)$ y los extremos absolutos ϕ y $(M \cup N)$.

1.292.

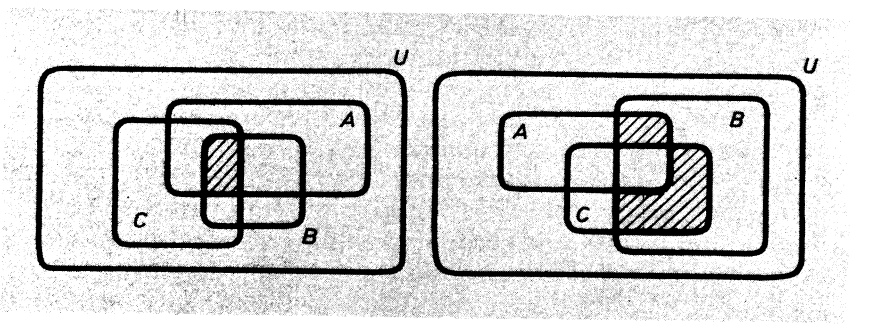
Reproduzca en su hoja de trabajo nueve veces el diagrama que se dibuja. Luego, raye en cada uno de ellos los resultados de las operaciones que se proponen:



$$A \cup B;\ A \cap B;\ A - B;\ B - A;\ B';\ A \triangle B;\ (A \cup B)';\ (B - A)';\ A' \cap B'$$

1.293.

Establézcanse las expresiones conjuntistas que pretenden representar estos diagramas:



1.294.

Justifíquese que si $\text{card}(A) = a$ y $\text{card}(B) = b$,

$$\text{card}(A \cup B) = a + b - \text{card}(A \cap B)$$

(Ayudará intentar la cuestión con diagramas de Venn.)

1.295.

Justifíquese gráfica y analíticamente que

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + \\ + n(A \cap B \cap C)$$

1.296.

Como aplicación, resuélvase este problema: A un simposio de la UNESCO, sobre contaminación del medio ambiente, asisten cien especialistas, de los cuales cincuenta hablan inglés, sesenta francés y cincuenta, español; de ellos, treinta hablan francés e inglés; veinte inglés y español; veinte francés y español. ¿Cuántos hablan los tres idiomas?

1.297.

Se sabe de *a* que es un número natural menor que 1 000; que no es par, que no es divisible por 5 y que no es múltiplo de 11. ¿Cuántos números *a*, con esas condiciones, pueden existir?

1.298.

Un «agente artístico» dispone a principio de temporada de veintinueve puestos de trabajo: trece, de señoritas para cuerpo de baile; otros trece, para pequeños papeles en varias películas, y quince, para coros de un gran espectáculo.

Para cubrir esas veintinueve colocaciones, interesa que seis señoritas puedan bailar en películas; cuatro, que puedan intervenir en un coro de películas, y cinco que sean capaces de cantar y bailar. Se pregunta:

1.º ¿Cuántas señoritas han de encontrarse que sean capaces de bailar, cantar e interpretar en el cine?;
2.º ¿cuántas muchachas que sólo sepan bailar se pueden contratar?;
3.º ¿y cuántas aspirantes a artistas han de saber bailar y cantar, pero no interpretar ante las cámaras?

1.299.

En demanda de trabajo llegan a la agencia artística del número anterior veintinueve muchachas con los siguientes «conocimientos»:

1.º quince con posibilidad de interpretar en el «plató»;
2.º dieciséis saben música suficiente para ser integrantes de un coro;
3.º seis señoritas saben bailar e interpretar en el cine;
4.º cinco aspirantes pueden cantar y hacer cine;
5.º Se comprobó que una era capaz de realizar las tres cosas.

Se pregunta: *a*) ¿cuántas bailarinas se presentaron?; *b*) ¿qué puestos no pueden cubrirse?; *c*) ¿qué solicitantes quedan sin trabajo?

1.3

Relaciones

1.31. Introducción

1.32. Relación binaria

1.321. *Descripción. Establecimiento*
1.322. *Representaciones*
1.323. *Propiedades*

1.33. Relación de equivalencia

1.331. *Definición*
1.332. *Acción de una relación de equivalencia*

1.3321. Clases de equivalencia
1.3322. Partición provocada por una equivalencia
1.3323. Conjunto cociente
1.3324. Representante canónico

1.34. Relación de orden

1.341. *Definición*
1.342. *Clases de ordenaciones*
1.343. *Primero y último elementos o elementos mínimo y máximo*

1.3431. Establecimiento
1.3432. Teorema

1.344. *Elementos maximal y minimal*
1.345. *Subconjuntos acotados*

1.3451. Mayorante o cota superior
1.3452. Minorante o cota inferior
1.3453. Elementos supremo e ínfimo

1.346. *Ordenes inversos*
1.347. *Retículos ordenados*

1.3471. Teorema «directo»
1.3472. Teorema «recíproco»

1.348. *Buena ordenación*

1.3481. Conjunto bien ordenado
1.3482. Teorema
1.3483. Axioma de elección. Postulado de Zermelo

1.35. El álgebra de las relaciones

1.351. *Igualdad y orden en el conjunto de las relaciones*
1.352. *Operaciones con relaciones*

1.3521. Unión o disyunción de relaciones
1.3522. Intersección o conjunción de relaciones
1.3523. Relaciones complementarias o negación de relaciones

1.353. *El álgebra de las relaciones*
1.354. *Producto de relaciones*

1.36. Aplicabilidad. Automatismos y destrezas

1.3

Relaciones

1.31. INTRODUCCION

La palabra «relación» y el concepto que describe es uno de los más usados en cualquier ámbito de comunicación y de cultura de los hombres.

Se dice (hoy, un tanto arcaico) que «Antonio y Carmen se han puesto en relaciones», para indicar el inicio de su noviazgo; que la empresa *A* y la empresa *B* están en «buenas relaciones» expresa la existencia de un amable quehacer común entre sus miembros; que el país *C* ha roto sus relaciones diplomáticas con el *D*, notifica que ya no existe «un lazo» que anteriormente existía entre los miembros de las dos comunidades políticas. Qué duda cabe de que Juan está relacionado de alguna manera con sus hijos Pedro y Luis; y de que los primos de éstos, Felipe y Ricardo, guardan relación estrecha con su padre, Carlos, hermano de Juan.

La extensión del concepto, así como su gran instrumentalidad, que se adivina, en la construcción de la ciencia (¡qué hubiera sido de Linneo —por ejemplo— sin este concepto) justifica sobradamente que se intente su matematización. En efecto, el concepto matemático de relación es uno de los más ricos y potentes de la ciencia: sin él —por ejemplo— no se podría *ordenar*, y no cabría hacer ninguna *clasificación*; no se podría dar, en fin, un solo paso en el camino del saber.

El niño que sonríe porque ha relacionado los ojos grandes de su madre con el pecho, el calor con la mano materna, ¿qué es, sino una primera clasificación?

1.32. RELACION BINARIA

1.321. Descripción. Establecimiento

Imagínese el conjunto de los siguientes autores universales:

$$A = \{\text{Homero, Sófocles, Virgilio, Cervantes, J. Hernández}\};$$

y éste, de obras maestras:

$$L = \{\textit{Ilíada}, \textit{Odisea}, \textit{Eneida}, \textit{Macbeth}, \textit{Don Quijote}, \textit{Fausto}, \textit{Martín Fierro}\}$$

En un test de cultura general, bien podría aparecer el siguiente ítem:

> «unir con flechas los nombres de la columna A que se relacionen con los de la columna L».

Nos encontramos frente a una relación binaria. Si el examinando ha dado una solución correcta, las flechas de su contestación habrán producido los siguientes *pares*:

> (Homero, *Ilíada*); (Homero, *Odisea*); (Virgilio, *Eneida*);
> (Cervantes, *Don Quijote*); (J. Hernández, *Martín Fierro*).

Puede observarse cómo la relación binaria produce unos pares del producto cartesiano de los conjuntos sobre los que actúa. En efecto, la relación R = «es autor de» ha seleccionado de todos los pares del cartesiano $A \times L$, aquellos para los que es cierta. Utilizando iniciales, podemos escribir:

$$(H\,R\,I);\ (H\,R\,O);\ (V\,R\,E);\ (C\,R\,Q);\ (Hz\,R\,MF)$$

De los $5 \times 7 = 35$ pares del cartesiano $A \times L$, la relación R ha determinado como ciertos los cinco expresados. Cualquiera de los otros treinta restantes no pertenecerían a la relación R, y serían fallos del examinando; y el que —por ejemplo— Sófocles no es autor de *Fausto*, se simboliza así:

$$(S\,\not{R}\,F)$$

Así, pues, dar una relación R entre dos conjuntos A y L equivale a establecer un grafo del cartesiano $A \times L$: el subconjunto de $A \times L$ para el que la relación es cierta.

La descripción sobre el ejemplo que hemos desarrollado permite abordar el establecimiento matemático del concepto.

Sean A y B dos conjuntos (finitos o no finitos, iguales o distintos), y sea p una proposición lógica sobre el cartesiano $A \times B$. Se denomina *relación* a la bina

$$[(A \times B)_{[1]},\ p]$$

en la que $(A \times B)_{[1]}$ expresa el conjunto de validez de la proposición p, sobre el cartesiano $(A \times B)$.

Si, como es frecuente, $A \equiv B$, entonces la relación R toma la expresión

$$[A^2_{[1]}, p]$$

Ejemplo 1

Sobre el conjunto A de las naciones sudamericanas se establece la relación R = «ser fronteriza con».

A = {Colombia, Ecuador, Perú, Chile, Argentina, Uruguay, Brasil, Guayana, Venezuela, Bolivia, Paraguay}

Usando iniciales, los $11^2 = 121$ pares del cartesiano son

$$A^2 = \{(C, C), (C, E), (C, Pe), \ldots, (Pa, Pa)\}$$

El grafo $G \subset A^2$ de R está formado por los cuarenta y siete pares, para los que R se verifica; así, por ejemplo,

$$(\text{Perú, Colombia}) \in G,$$

y

$$(\text{Chile, Ecuador}) \notin G,$$

lo que puede expresarse

$$(\text{Perú } R \text{ Colombia}) \quad \text{y} \quad (\text{Chile } \not R \text{ Ecuador}).$$

Queda establecido de este modo que Perú es fronteriza con Colombia; y que Chile no lo es con Ecuador.

Ejemplo 2

Sea M el conjunto de todas las rectas del plano euclídeo; y sea la relación R = «es paralela a».

Si $r_1 \in M$ y $r_2 \in M$, puede suceder que $r_1 \,//\, r_2$ o que $r_1 \not// r_2$. En el primer caso, $(r_1, r_2) \in G$; en el segundo, $(r_1, r_2) \notin G$.

Otra relación en M podría ser P = «es perpendicular a». Y para dos rectas del plano podría ser que $r_1 \perp r_2$ o que $r_1 \not\perp r_2$, lo que equivaldría a escribir que

$$(r_1, r_2) \in G \quad \text{o que} \quad (r_1, r_2) \notin G.$$

NOTA. Como se ha podido observar en los ejemplos, no siempre se utiliza la letra R (o cualquiera otra que pudiera establecerse) para intercalar entre los elementos que están relacionados. A veces (y suelen ser los casos más interesantes) la relación tiene nombre y signo propios, consagrados por el uso. Así sucede con las relaciones de paralelismo (//) y perpendicularidad ($\perp$), a que hemos aludido anteriormente. Otras que ya se han tenido ocasión de utilizar, son: la relación de inclusión ($\subset$), la de pertenencia ($\in$), la de implicación ($\Rightarrow$), la de equivalencia lógica ($\Leftrightarrow$) y la primigenia de todas, la de igualdad ($=$).

1.322. Representaciones

Es cómodo, a veces, para establecer una relación entre conjuntos finitos, disponer una representación gráfica, resultando las más usadas, la representación cartesiana y la matriz de números.

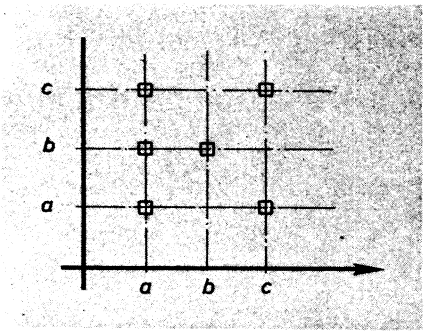
Siendo un grafo un subconjunto de un cartesiano, la técnica de representación es idéntica a la que allí se empleó, resultando aquí que no todos los nudos de la red están marcados, sino solamente los del conjunto de validez de R; a saber: los de su grafo.

La otra forma de representación, la matriz de números, se construye registrando en un cuadro de doble entrada, 1, si el par a que corresponde la casilla pertenece G; 0, si el par no pertenece a la relación.

Sea el conjunto $A = \{a, b, c\}$ y una relación R sobre él, cuyo grafo es

$$A^2 \supset G = \{(a, a),\ (a, b),\ (b, b),\ (a, c),\ (c, c),\ (c, a)\}.$$

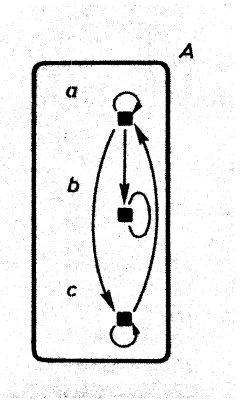
He aquí dos representaciones:



R	a	b	c
a	1	0	1
b	1	1	0
c	1	0	1

NOTA. Se conviene en leer las primeras proyecciones de cada par en el eje (en la entrada) horizontal.

Digamos finalmente, que si el conjunto A sobre el que actúa la relación R está representado mediante un diagrama de Venn, entonces los pares de su grafo se resaltan mediante flechas que, saliendo de cada primera proyección, terminan en la segunda correspondiente. Así:



1.323. Propiedades

Las relaciones binarias pueden tener, entre otras, las siguientes propiedades:

Reflexividad: Se dice que la relación $[A^2_{[1]}, p]$ es reflexiva, si todo elemento de A está relacionado consigo mismo: $\forall a \in A,\ a\,R\,a$; o lo que es igual:

$$[A^2_{[1]}, p] \text{ es reflexiva} \Leftrightarrow \forall a \in A,\ (a, a) \in A^2_{[1]}$$

Las representaciones gráficas de una R reflexiva presentan ocupados todos los nudos de la bisectriz del cuadrante o la diagonal de su matriz de números está ocupada en su totalidad por 1; y si se trata de un diagrama de Venn, todos los elementos presentan un «bucle».

Ejemplo 1

La relación de amistad, «ser amigo de», sobre el conjunto de los humanos, es una relación reflexiva*.

Ejemplo 2

La relación «ser menor o igual que», sobre el conjunto de los naturales, es una relación reflexiva, pues

$$\forall x \in N, \qquad x \leq x$$

Ejemplo 3

La relación de paternidad, «ser padre de» sobre el conjunto de los miembros de una familia no es reflexiva, pues nadie es padre de sí mismo.

Ejemplo 4

La relación «ser menor que», sobre el conjunto de los naturales, no es reflexiva. En efecto:

$$\forall x \in N, \qquad x \not< x$$

Simetría: La relación $[A^2_{[1]}, p]$ es simétrica, si el hecho de que $a\,R\,b$ implica que $b\,R\,a$. Es decir:

$$[A^2_{[1]}, p] \text{ es simétrica} \Leftrightarrow \forall (a, b) \in A^2_{[1]},\ \exists (b, a) \in A^2_{[1]}$$

La simetría de una relación se denuncia en las gráficas porque «doblando» por la bisectriz del cuadrante (por la diagonal de la matriz), han de coincidir los nudos (los «1») de la red (de la matriz), de un lado y de otro de la bisectriz (de la diagonal). Si de diagramas de Venn se trata, la simetría de R se pone de manifiesto porque todo par de elementos relacionados han de tener «flechas de ida y vuelta».

---

* Si se ha de dar crédito al aforismo sanchopancesco, «El amor, bien entendido, ...».

Ejemplo 5

La relación de amistad no es simétrica, pues —por desgracia— el que A sea amigo de B, no siempre implica que B sea amigo de A.

Ejemplo 6

La relación $[N^2_{[1]}, \leq]$ no es simétrica, pues

$$\forall (x, y) \in N^2_{[1]} \not\Rightarrow (y, x) \in N^2_{[1]} \qquad [1]$$

Ejemplo 7

La relación de hermandad sobre los miembros de una familia sí es simétrica, pues si A es hermano de B, B es hermano de A.

Ejemplo 8

La relación de congruencia (dar el mismo resto al dividir por m) sobre el conjunto Z sí es simétrica, pues si el entero x da de resto r al dividir por m y el y, también, es claro que y da el mismo resto r que x, al dividir por m:

$$x \equiv y \ (m \Leftrightarrow y \equiv x \ (m$$

Transitividad: La relación $[A^2_{[1]}, p]$ es transitiva, si sucede que $x \in A$, $y \in A$, $z \in A$, $\left.\begin{matrix} x\,R\,y \\ y\,R\,z \end{matrix}\right\} \Rightarrow x\,R\,z$; o más correctamente,

$$[A^2_{[1]}, p] \text{ es transitiva} \Leftrightarrow [(x, y) \in A^2_{[1]} \wedge (y, z) \in A^2_{[1]}] \Rightarrow (x, z) \in A^2_{[1]}$$

Ejemplo 9

La relación de amistad, obviamente, no es transitiva. A y B pueden ser amigos y B y C, también; y, sin embargo, es posible que A y C no se conozcan.

Ejemplo 10

La relación de orden «ser menor que», sobre el conjunto de los naturales, es transitiva, pues

$$[(x\,y) \in N^2_{[1]}] \wedge [(y, z) \in N^2_{[1]}] \Rightarrow (x, z) \in N^2_{[1]},$$

que equivale a escribir:

$$(x < y) \wedge (y < z) \Rightarrow (x < z)$$

Antisimetría: La relación $[A^2_{[1]}, p]$ se dice que es antisimétrica si $x \in A$, $y \in A$,

$$[(x\,R\,y) \wedge (y\,R\,x)] \Rightarrow x \equiv y$$

o bien,

$$[A^2_{[1]}, p] \text{ es antisimétrica} \Leftrightarrow [(x, y) \in A^2_{[1]} \wedge (y, x) \in A^2_{[1]}] \Rightarrow x \equiv y$$

Tal vez esta propiedad presente cierta dificultad de interpretación y, por ende, alguna explicación. Para ello, vamos a valernos de una relación de orden, ya conocida, muy importante: la de inclusión sobre el conjunto-potencia de un determinado conjunto.

Supóngase que se ha conseguido probar que el conjunto A está incluido en el B; y que, por otro camino, se ha demostrado fehacientemente que el conjunto B es subconjunto de A. Pues bien; si esto es así, la conclusión es inmediata: se trata del mismo conjunto.

$$[(A \subset B) \wedge (B \subset A)] \Rightarrow A \equiv B$$

La relación de inclusión —queda claro— es una relación antisimétrica.

Abundemos un poco en esta cuestión con el

Ejemplo 11

Sea ahora el conjunto de los Reyes Godos españoles, y sobre él, la relación «ser posterior a».

De un rey del que no se conoce su nombre, que denotaremos W, se ha investigado que fue posterior a otro S, del que se han determinado sus hazañas y decretos, pero no su identidad.

Otros investigadores han alcanzado a establecer, sin ninguna duda, que el rey que hizo las hazañas que hizo S es posterior al que hemos dado en llamar W.

Si todo esto es así, es evidente que los innominados W y S son la misma persona; se trata del mismo rey:

$$\left.\begin{array}{l} W \text{ es posterior a } S \\ S \text{ es posterior a } W \end{array}\right\} \Rightarrow W \text{ es } S$$

1.33. RELACION DE EQUIVALENCIA

1.331. Definición

La relación $[A^2_{[1]}, p]$ es una relación de equivalencia, si es reflexiva, simétrica y transitiva. A saber:

$$\left.\begin{array}{l} (A^2_{[1]}, p) \text{ es} \\ \text{relación de} \\ \text{equivalencia} \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} \forall x \in A,\ (x, x) \in A^2_{[1]} \\ (x, y) \in A^2_{[1]} \Leftrightarrow (y, x) \in A^2_{[1]} \\ (x, y) \in A^2_{[1]} \wedge (y, z) \in A^2_{[1]} \Rightarrow (x, z) \in A^2_{[1]} \end{array}\right.$$

Ejemplo

La relación de paralelismo sobre las rectas del plano es una relación de equivalencia. En efecto:

1) $\forall r \in M,\ r // r$
2) $r \in M,\ s \in M,\ r // s \Leftrightarrow s // r$
3) $r \in M,\ s \in M,\ t \in M,$

$$\left.\begin{matrix} r // s \\ s // t \end{matrix}\right\} \Rightarrow r // t$$

No así la relación de perpendicularidad sobre el mismo conjunto, pues ni es reflexiva ni transitiva

1) $\forall\, r \in M,\ r \not\perp r$
3) $r \in M,\ s \in M,\ t \in M,$

$$\left.\begin{matrix} r \perp s \\ s \perp t \end{matrix}\right\} \Rightarrow r // t \qquad \text{y no} \qquad r \perp t$$

1.332. Acción de una relación de equivalencia

La relación de equivalencia constituye un instrumento de matematización de gran eficacia. En efecto, es capaz de crear nuevos objetos matemáticos, al actuar sobre un conjunto.

Hasta concluir cuál es su acción, se desarrolla el tema en varios subepígrafes.

1.3321. *Clases de equivalencia*

Establecido un conjunto A y sobre él una relación de equivalencia R, considérense los subconjuntos de A, formados por todos los elementos equivalentes a cada uno de los $a \in A$.

$$[a] = \{x/(x \in A) \wedge (x\ R\ a)\}$$

Estos subconjuntos, así formados, se llaman «clases de equivalencia» o, simplemente, «clases».

Ejemplo

Desde Elda —emporio del calzado español— se intenta exportar a Estados Unidos cincuenta mil pares de zapatos.

La caja cuya referencia es P-54/37 contiene un par de zapatos de piel; la N-12/35 guarda un par de napa; la A-13/36 tiene dentro zapatos de ante; y la S-5/40 resulta contener un par fabricado con piel sintética.

Todos los pares de zapatos que, como los de la primera referencia, son de piel, *forman* la clase «piel»; todos los fabricados con napa, constituyen la clase «napa»;

los construidos con el material de los de la caja A-13/36 forman la clase «ante»; y todos los de referencia S son elementos de la clase «piel sintética».

Sobre el conjunto Z de zapatos a exportar, la relación R = «estar construidos con el mismo material», ha producido las clases de equivalencia

$$\{\text{piel}\},\ \{\text{napa}\},\ \{\text{ante}\},\ \{\text{piel sintética}\}$$

1.3322. *Partición provocada por una equivalencia*

Las clases producidas por una relación de equivalencia sobre A forman una partición en A. En efecto:

1.º Forman un *recubrimiento* de A, es decir:

$$\cup[a] \equiv A$$

Para demostrarlo, basta justificar que todo elemento de A pertenece a una de esas clases.

Sea un $b \in A$, y considérese la clase

$$[b] = \{x/(x \in A) \wedge (x\ R\ b)\}$$

Que $b \in [b]$ es evidente, ya que por ser R reflexiva, $b\ R\ b$.

2.º Dos clases cualesquiera son siempre *disjuntas*, o sea:

$$[a] \cap [b] = \phi$$

Demostremos por reducción al absurdo. Admitamos que existe un c que pertenece a dos clases distintas, $[a]$ y $[b]$.

$$\left.\begin{array}{r} c \in [a] \Rightarrow c\ R\ a \Rightarrow a\ R\ c \\ c \in [b] \Rightarrow c\ R\ b \end{array}\right\} \Rightarrow a\ R\ b \Leftrightarrow b\ R\ a$$

$$\left.\begin{array}{r} \forall d \in [a] \Rightarrow d\ R\ a \\ a\ R\ b \end{array}\right\} \Rightarrow d\ R\ b \Rightarrow d \in [b] \Rightarrow [a] \subset [b] \qquad [1]$$

$$\left.\begin{array}{r} \forall e \in [b] \Rightarrow e\ R\ b \\ b\ R\ a \end{array}\right\} \Rightarrow e\ R\ a \Rightarrow e \in [a] \Rightarrow [b] \subset [a] \qquad [2]$$

De [1] y [2] se sigue que las clases $[a]$ y $[b]$, que tienen un c común, son la misma, contra lo supuesto; entonces,

$$[a] \equiv [b]$$

Así, resulta que toda relación de equivalencia sobre un conjunto provoca una partición en subconjuntos, llamados «clases». Por esta razón, estas particiones, creadas *a posteriori* por la acción de una relación de equivalencia, se llaman *clasificaciones*.

Recíprocamente, es fácil probar que toda partición en A, realizada *a priori*, lleva consigo una clasificación. En efecto:

Sea la partición

$$A \equiv A_1 + A_2 + \cdots + A_n$$

Establezcamos una relación R sobre A, cuyo predicado sea p = «pertenecer a la misma parte de A»; o sea:

$$a \in A,\ b \in A,\ a\,R\,b \Leftrightarrow (a \in A_i) \wedge (b \in A_i).$$

Demostremos que se produce una clasificación, justificando que la R establecida es de equivalencia:

R es reflexiva:	$a\,R\,a, \quad \forall a \in A$	Evidente
R es simétrica:	$a\,R\,b \Leftrightarrow b\,R\,a$	Inmediato
R es transitiva:	$\left.\begin{matrix} a\,R\,b \\ b\,R\,c \end{matrix}\right\} \Rightarrow a\,R\,c$	

$$(a \in A_i) \wedge (b \in A_i) \wedge (c \in A_i) \Rightarrow (a \in A_i) \wedge (c \in A_i) \Rightarrow a\,R\,c$$

1.3323. *Conjunto cociente*

El conjunto de todas las clases, que denotaremos

$$A/R = \{[x]/[x] = \{y/(y \in A) \wedge (y\,R\,x)\}\}$$

se denomina *conjunto-cociente.*

NOTA 1. Considérese que, como consecuencia inmediata de la definición, ninguna clase puede ser vacía.

NOTA 2. Adviértase que los elementos de A/R son, a su vez, conjuntos.

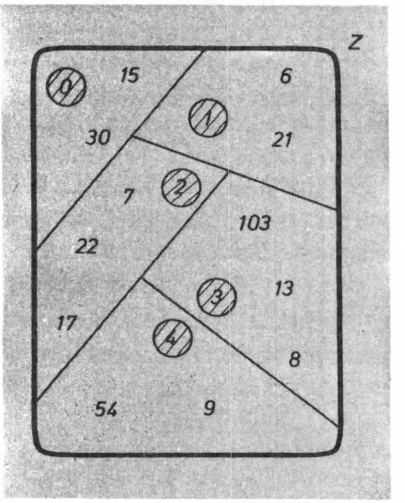
Ejemplo 1

Sea F el conjunto de jugadores de fútbol, federados en la primera división del Campeonato Nacional de Liga, 1975/76. Y sea la relación de equivalencia R = «pertenecer al mismo club».

Esta relación R *clasifica* al conjunto de jugadores en subconjuntos disjuntos, cada uno de los cuales es un club de primera división. De modo que el conjunto cociente, F/R, resulta ser el conjunto de los clubs de la división «de honor».

Ejemplo 2

Sea Z el conjunto de los números enteros y la relación de congruencia, módulo 5, que denotaremos $\equiv$ (véase ejemplo 8, de 1.323). Interprétese el diagrama de Venn, que se dibuja. De este modo, Z ha quedado *clasificado* en cinco clases de equivalencia (llamadas aquí «clases residuales»), por la relación de congruencia, *módulo* 5.



1.3324. *Representante canónico*

Para manejar la clase que produce una R de equivalencia, resultaría engorroso, y aun imposible, referirse a ellas en su totalidad (no se olvide que se trata de conjuntos que pueden llegar a ser no finitos). Para obviar esta dificultad, se conviene en crear el llamado representante canónico.

Recibe este nombre el elemento de cada clase $[a]$, escogido para representarla.

Claro es que debe escogerse el más sencillo, cuando esto sea posible.

En el ejemplo 1 del número anterior, es preceptivo que, si el árbitro ha de comunicar alguna cuestión a un equipo, lo ha de hacer no reuniendo «en corro» a todos sus jugadores, sino hablando con su representante «canónico»: el capitán.

En el segundo ejemplo, se tomarán como representantes de cada clase residual, módulo 5, el resto más pequeño, de modo que el conjunto-cociente resulta así:

$$Z/5 = \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}\},$$

en el que $\{0\}$ representa todos los enteros múltiplos de 5;
$\{1\}$ representa todos los enteros del tipo $5k + 1$;
$\{2\}$ representa todos los enteros del tipo $5k + 2$;
$\{3\}$ representa todos los enteros del tipo $5k + 3$;
$\{4\}$ representa todos los enteros del tipo $5k + 4$.

Se tituló este epígrafe «acción de una relación de equivalencia»; concluyamos escribiendo:

> Una relación de equivalencia R sobre A, *clasifica y parte* a A en subconjuntos disjuntos, cada uno de los cuales es una *clase* de equivalencia.
> El conjunto de las clases es el *conjunto-cociente*.

1.34. RELACION DE ORDEN

1.341. Definición

La relación $[A^2_{[1]}, p]$ es una relación de orden amplio o, simplemente, de orden, si es reflexiva, antisimétrica y transitiva. O sea:

$$[A^2_{[1]}, p] \text{ es relación de orden} \Leftrightarrow \begin{cases} 1)\ \forall x \in A \quad , \quad (x, x) \in A^2_{[1]} \\ 2)\ (x, y) \in A^2_{[1]} \wedge (y, x) \in A^2_{[1]} \Rightarrow x \equiv y \\ 3)\ (x, y) \in A^2_{[1]} \wedge (y, z) \in A^2_{[1]} \Rightarrow (x, z) \in A^2_{[1]} \end{cases}$$

Dispuesta la letra representativa de la relación entre los elementos que relaciona, se leerá «precede a», o bien «es antecedente de» y otras veces, «es anterior a», de un modo genérico.

Como sucedía en las relaciones de equivalencia, existen muchas de orden, con símbolos y nombres propios. Ocasiones sobradas habrá en este desarrollo de referirnos a ellas.

Ejemplo 1

Si se dice que el conjunto A está ordenado mediante la relación Ω, se escribirá (A, Ω) para indicar el conjunto ordenado; y si en algún momento se establece que $a\ \Omega\ b$, se está indicando que

a es anterior a b;
a precede a b;
a es antecedente de b,

en el orden establecido (A, Ω).

Ejemplo 2

La relación de inclusión en el conjunto de las partes de A, $P(A)$, es una relación de orden amplio, por cumplir las tres propiedades de su definición.

Ejemplo 3

La implicación lógica en el conjunto de las proposiciones es una relación de orden, ya que es reflexiva, antisimétrica y transitiva.

1.342. Clases de ordenaciones

Una relación Ω, reflexiva, antisimétrica y transitiva, ya se ha establecido como una relación de *orden amplio*; si Ω no es reflexiva, pero sí antisimétrica y transitiva, se dice que es una relación de *orden estricto*.

El hecho de que una relación Ω sea reflexiva y transitiva permite calificarle de

preordenación. Es claro, entonces, que tanto las relaciones de equivalencia como las de orden amplio son preordenaciones.

De otro lado, en función de que la relación de orden afecte o no a todo par del conjunto que ordena, existen dos clases de órdenes: *orden parcial* y *orden total.* Se dirá de (A, Ω) que es un orden total, si, para dos cualesquiera elementos, a, b, de A, puede escribirse que $a \,\Omega\, b$ o bien, que $b \,\Omega\, a$; o sea, que todo par de elementos es comparable. Simbólicamente,

$$\text{el orden } (A, \Omega) \text{ es total} \Leftrightarrow (\forall x \in A) \wedge (\forall y \in A) \Rightarrow [(x, y) \in A^2_{[1]} \vee (y, x) \in A^2_{[1]}]$$

Se establecerá el orden (A, Ω) como parcial si la relación Ω no relaciona todos los pares de proyecciones intercambiadas, de A^2. O sea, que, dados dos elementos a y b de A, no siempre puede decirse que «a precede a b» o que «b precede a a». En fin: no todos los elementos son comparables.

Ejemplo 1

El orden $(N, \leq)$ es un orden amplio, pues, para cualquier natural a, puede escribirse que

$$a \leq a,$$

que es la expresión de la reflexibilidad.

Además, la relación $\leq$, sobre N, es antisimétrica y transitiva. (Compruébese.)

También $(N, \leq)$ es un orden total, ya que, dados dos números naturales a y b, siempre se puede escribir que

$$a \leq b \quad \text{o} \quad b \leq a$$

Ejemplo 2

El orden $(N, <)$ es un orden estricto, pues la relación «menor que» no es reflexiva en N. En efecto: no es cierto que, siendo a un natural, a sea menor que a:

$$a \nless a$$

(Justifíquese que es antisimétrica y transitiva.)

Ejemplo 3

La relación de inclusión sobre el conjunto de las partes de A forma un orden $[P(A), \subset]$ amplio, parcial, pues es reflexiva, antisimétrica y transitiva, pero no siempre dos subconjuntos de A son comparables.

Ejemplo 4

La relación de divisibilidad, x/y («x divide a y») sobre los naturales produce el orden $(N, x/y)$, amplio y parcial; amplio, porque todo natural es divisor de sí

mismo (reflexividad); parcial, porque, dados dos naturales a y b, no siempre se podrá establecer que

$$a/b \quad \text{o que} \quad b/a$$

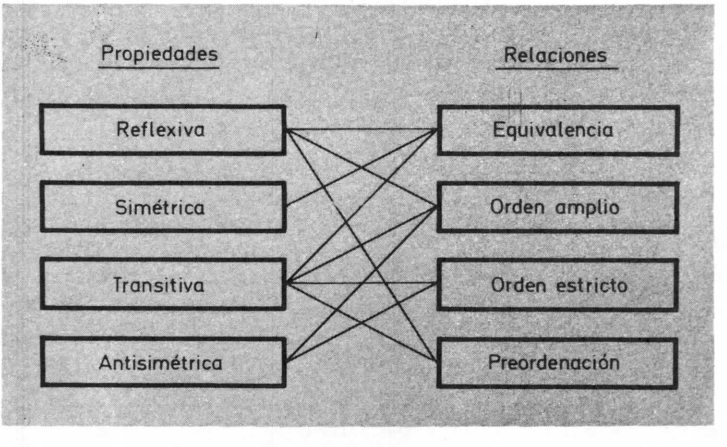
Ejemplo 5

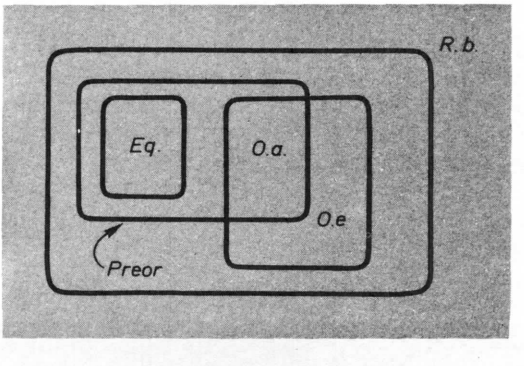
Sin embargo, la relación de divisibilidad, x/y, sobre el conjunto de los números enteros, Z, no es una relación de orden, ya que no goza de la propiedad antisimétrica. En efecto:

$$\left.\begin{matrix}(+a)/(-a)\\(-a)/(+a)\end{matrix}\right\} \Rightarrow (+a \not\equiv (-a)$$

No obstante, la relación sí es reflexiva y transitiva, por lo que $(Z, x/y)$ es una *preordenación*, de acuerdo con la nomenclatura establecida antes.

Tal vez sea bueno resumir en un cuadro toda la terminología expuesta hasta el momento. Además, con un diagrama de Venn, se muestran las diversas inclusiones de los conceptos tratados.





1.343. Primero y último elementos o elementos mínimo y máximo

1.3431. *Establecimiento*

Sea el orden (A, Ω). Se denomina primer elemento o *mínimo* de ese orden a un elemento $a \in A$, tal que para todo $x \in A$, a precede a x; es decir

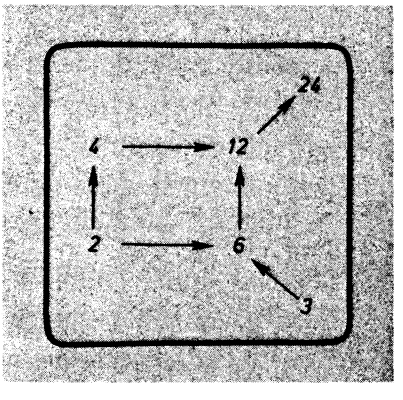
$$\left.\begin{array}{l} a \in A \text{ es mínimo} \\ \text{de } (A, \Omega) \end{array}\right\} \Leftrightarrow \forall x \in A,\ a\,\Omega\,x$$

De análoga manera, llamaremos último elemento o *máximo* del orden (A, Ω) a un $b \in A$, tal que sea posterior a todo elemento de A; o sea

$$\left.\begin{array}{l} b \in A \text{ es máximo} \\ \text{de } (A, \Omega) \end{array}\right\} \Leftrightarrow \forall x \in A,\ x\,\Omega\,b$$

Ejemplo 1

Sea el orden parcial de divisibilidad $(A, x/y)$ sobre el conjunto $A = \{2, 3, 4, 6, 12, 24\}$. El diagrama de ese orden es



$(A, x/y)$

Este orden no tiene primer elemento; ningún elemento de A divide a todos los demás.

Su último elemento es 24, ya que todo elemento de A le divide.

Ejemplo 2

El orden $(N, \leq)$ tiene como primer elemento el 1; pero no tiene último elemento.

Ejemplo 3

El subconjunto de los racionales $Q_1 = \{x/(x \in Q) \wedge (0 < x < 1)\}$ ordenado con la relación $\leq$, no tiene ni mínimo ni máximo, pues dado cualquier racional de Q_1, siempre se puede encontrar uno superior y otro inferior a él, dentro de Q_1.

Ejemplo 4

El sunconjunto de los racionales $Q_2 = \{x/(x \in Q) \wedge (0 < x \leq 1)\}$ tiene último elemento (máximo), que es el 1, en el orden $(Q_2, \leq)$; pero no tiene primer elemento (mínimo). Si se trata de ordenar con la relación $\leq$ el subconjunto de los racionales $Q_3 = \{x/(x \in Q) \wedge (0 \leq x < 1)\}$, ahora sí hay primer elemento, pero no último.

Si el conjunto a ordenar es el $Q_4 = \{x/(x \in Q) \wedge (0 \leq x \leq 1)\}$, entonces el 0 es el primer elemento y el 1, el último.

1.3432. TEOREMA. En un orden parcial, el primero y último elementos, si existen, son únicos.

Justifiquemos el teorema por reducción al absurdo, para el elemento máximo.

Admítase que existen dos elementos máximos, a_1 y a_2, distintos. Según la definición, se deberá cumplir

$$\begin{array}{lll} \forall x \in A, \ x \,\Omega\, a_1; & \text{en particular,} & a_2 \,\Omega\, a_1 \\ \forall x \in A, \ x \,\Omega\, a_2; & \text{en particular,} & a_1 \,\Omega\, a_2 \end{array}$$

La antisimetría de la relación Ω, permite la implicación

$$\left.\begin{array}{l} a_2 \,\Omega\, a_1 \\ a_1 \,\Omega\, a_2 \end{array}\right\} \Leftrightarrow a_1 \equiv a_2,$$

contra hipótesis; luego la tesis es correcta.

Ejercítese el lector, justificando análogamente, la unicidad del elemento mínimo.

1.344. Elementos maximal y minimal

Sea el orden parcial (A, Ω). Se dice que $a \in A$ es *maximal*, si no existe en A ningún otro elemento posterior a a, en sentido estricto. O sea:

$$\forall x \in A, \quad a \,\Omega\, x \Rightarrow a \equiv x$$

Análogamente, se dice que b es minimal de (A, Ω), si no existe en A ningún otro elemento anterior a él, en sentido estricto. Simbólicamente:

$$\forall x \in A, \quad x \,\Omega\, b \Rightarrow b \equiv x$$

Ejemplo

Considérese de nuevo el orden establecido en el primer ejemplo del párrafo 1.3431.

En ese orden, 24 es un elemento maximal, pues a ninguno, excepto a sí mismo, divide. Ninguno de los elementos de A puede reemplazarse por x en la expresión

$$24 \,\Omega\, x \qquad \text{(léase «24 divide a } x\text{»)}.$$

Los elementos 2 y 3 son minimales de $(A, x/y)$. En efecto: ningún elemento de A, excepto 2, divide a 2; asimismo, ningún elemento divide a 3. No es posible escribir

$$x \,\Omega\, 2 \quad \text{ni} \quad x \,\Omega\, 3,$$

para ningún $x \in A$.

1.345. Subconjuntos acotados

1.3451. *Mayorante o cota superior*

Sea el orden (A, Ω) y $B \subset A$. Se denomina mayorante o cota superior de B a todo elemento de A, que denotamos m, tal que, para todo $x \in B$, sucede que x precede a m. Es decir:

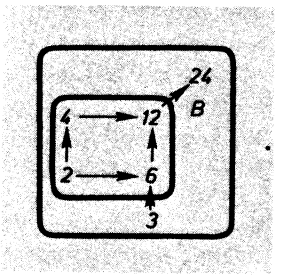
$$\left.\begin{array}{l} m \in A \text{ es mayorante} \\ \text{de } B \subset A \end{array}\right\} \Leftrightarrow \forall x \in B, \quad x \,\Omega\, m$$

Ejemplo

Repitamos aquí el diagrama de orden del primer ejemplo del párrafo 1.3431 y consideremos el subconjunto $B = \{2, 4, 6, 12\}$.

El conjunto de mayorantes de B es

$$M_{(B)} = \{12, 24\}$$



$(A, x/y)$

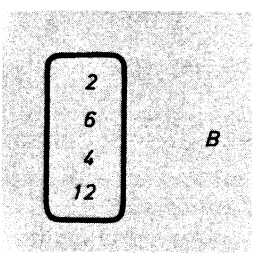
1.3452. *Minorante o cota inferior*

Sea el orden (A, Ω) y $B \subset A$. Se dice que un $n \in A$ es minorante de B si todo elemento de B es posterior a n. O sea:

$$\left.\begin{array}{l} n \in A \text{ es minorante} \\ \text{de } B \subset A \end{array}\right\} \Leftrightarrow \forall x \in B, \quad n \,\Omega\, x$$

Siguiendo con nuestro ejemplo, digamos que el único minorante de B es 2, pues sólo con él se puede escribir que

2 divide a
2 divide a
2 divide a
2 divide a



Escribimos entonces, $N_{(B)} = \{2\}$.

Un conjunto que posee cotas superiores o mayorantes se dice que está *acotado superiormente*; si su conjunto de minorantes o cotas inferiores no es el conjunto vacío, se trata de un conjunto *acotado inferiormente*. Si se trata de un conjunto que tiene tanto cotas superiores como inferiores se habla, simplemente, de un conjunto *acotado*.

El conjunto B del ejemplo que venimos estableciendo es un conjunto acotado.

1.3453. *Elementos supremo e ínfimo*

Considérese el orden (A, Ω) y sea un $B \subset A$, acotado. Los conjuntos de sus cotas superiores o mayorantes y el de sus cotas inferiores o minorantes se denotan, respectivamente, $M_{(B)}$ y $N_{(B)}$.

Establezcamos los órdenes $(M_{(B)}, \Omega)$ y $(N_{(B)}, \Omega)$.

Se denomina *extremo superior* o *supremo de B* al mínimo —si existe— del conjunto de sus mayorantes. Se denota $\overline{\text{ext}}(B)$ o $\sup(B)$.

> (Si el orden genérico, Ω, se particulariza para $\leq$, puede traducirse la definición como «la menor de sus cotas superiores».)

De análoga manera, se dirá que $\underline{\text{ext}}(B)$ o $\inf(B)$ es el *extremo inferior* o *ínfimo de B*, si es el elemento máximo —si existe— del conjunto de sus minorantes o cotas inferiores.

> (Si al igual que antes, el orden del que se trata es $\leq$, puede establecerse el concepto, diciendo que «es la mayor de sus cotas inferiores».)

Cuando el $\sup(B)$ o/y el $\text{ínf}(B)$ pertenecen al subconjunto B, se acostumbra a decir que son *accesibles*, siendo *inaccesibles*, en caso contrario.

Adviértase que el $\sup(B)$ accesible coincide con el máximo o último elemento de B; de igual modo, el $\inf(B)$, de ser accesible, es el mínimo o primer elemento del conjunto B.

Ejemplo 1

Continuando con el ejemplo de divisibilidad que venimos desarrollando,

12 es el $\sup(B)$, accesible, y coincide con $\text{máx}(B)$;
2 es el $\inf(B)$, accesible, y coincide con $\text{mín}(B)$.

Ejemplo 2

Sea el subconjunto de los racionales positivos

$$Q_5 = \{x/(x \in Q^+) \wedge (2 < x^2 < 3)\}$$

Se desean determinar —si existen— los extremos superior e inferior del orden $(Q_5, \leq)$; es decir: $\sup(Q_5)$ e $\inf(Q_5)$.

Analicemos, primero, si es un conjunto acotado.

a) *superiormente*: efectivamente, posee un conjunto no finito de mayorantes:

$$M_{(Q_5)} = \{x/(x \in Q^+) \wedge (x^2 \geq 3)\};$$

b) *inferiormente*:
es claro que Q_5 es un conjunto «minorado» en Q^+, ya que sus minorantes o cotas inferiores son infinitas:

$$N_{(Q_5)} = \{x/(x \in Q^+) \wedge (x^2 \leq 2)\}$$

Establecido que —en efecto— se trata de un conjunto acotado, pasemos a analizar si posee extremos.

El $\sup(Q_5)$, su extremo superior, habría de ser el primer elemento (mínimo) de $M_{(Q_5)}$; pero este conjunto de mayorantes no tiene primer elemento:

$(Q_5, \leq)$ no tiene extremo superior:

$$\nexists \sup(Q_5)$$

El $\inf(Q_5)$, su extremo inferior, sería el último elemento (máximo) de $N_{(Q_5)}$; pero ese conjunto de sus minorantes no posee máximo o último elemento

$(Q_5, \leq)$ no tiene extremo inferior:

$$\nexists \inf(Q_5)$$

NOTA. Cáigase en la cuenta de que $\sqrt{2}$ y $\sqrt{3}$ no pertenecen a Q_5; ni siquiera a Q^+; no son racionales.

1.346. Ordenes inversos

En espera de que en el punto 1.35 se trate cumplidamente, y de un modo general, el álgebra de las relaciones, es bueno dejar apuntado aquí la cuestión que titula el epígrafe. Por lo demás —y hasta entonces—, que la intuición supla, por ahora, lo que luego se construirá y estructurará debidamente, no parece nocivo.

Es fácil demostrar que si Ω es una relación reflexiva, antisimétrica y transitiva, su recíproca Ω^{-1} también lo es, y el orden parcial que pueda establecer sobre un conjunto A, (A, Ω^{-1}) es el llamado *orden inverso* del (A, Ω).

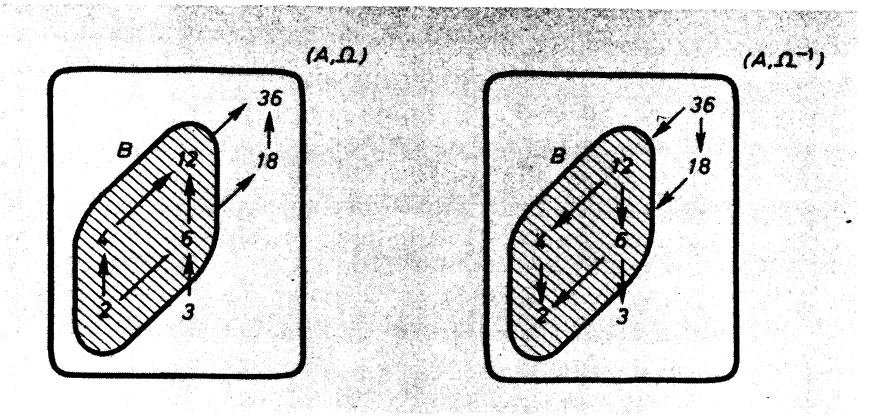
En los diagramas de orden, los órdenes inversos se denuncian por el cambio de sentido de las flechas.

Todos los conceptos referibles al orden (A, Ω) se intercambian con los correspondientes, referidos al inverso (A, Ω^{-1}). Así, primero y último elementos, mayorantes y minorantes de algún $B \subset A$, etc.

Ejemplo

Sea sobre $A = \{2, 3, 6, 4, 12, 18, 36\}$ la relación Ω = «ser divisor de». La Ω^{-1} es «ser múltiplo de».

Los diagramas de los órdenes correspondientes son:



El orden (A, Ω) no posee primer elemento; su último elemento es 36.
El primer elemento de (A, Ω^{-1}) es 36; no tiene último elemento.
Los elementos minimales de (A, Ω) son 2 y 3; 36 es su maximal.
Los elementos maximales de (A, Ω^{-1}) son 2 y 3; 36 es su minimal.

Si se considera ahora el subconjunto $B = \{2, 4, 6, 12\}$, en el orden (A, Ω) sus mayorantes son $M_{(B)} = \{12, 36\}$ y $\sup(B) = 12$; sus minorantes son $N_{(B)} = \{2\}$ e $\inf(B) = 2$.

Pues bien: si es (A, Ω^{-1}) el orden considerado, sucede que

$$M_{(B)} = \{2\} \text{ y } \sup(B) = 2$$
$$N_{(B)} = \{36, 12\} \text{ e } \inf(B) = 12$$

1.347. Retículos ordenados

Al hablar de la Teoría de Conjuntos, ya quedó indicado que el conjunto de las partes de A, con las operaciones unión e intersección, tenía estructura de retículo, por cumplir las leyes de

T_1) Absorción,
T_2) Idempotencia,
T_3) Asociatividad y
A_4) Conmutatividad.

De la misma manera, en la página 18 y en la 32 se decía que el conjunto de las proposiciones lógicas, con las operaciones de disyunción y conjunción formaban, también, un retículo, pues se cumplían las mismas leyes.

Ambos casos no son más que concreciones de la misma estructura matemática: el álgebra de Boole, que se presenta en el capítulo 2.1.

Pues bien: los teoremas que siguen se refieren a los términos recordados. Utilizaremos simbología conjuntista, aunque bien puede comprender el lector con *lo dicho* que el tratamiento es general.

1.3471. TEOREMA *«directo»*

Todo retículo es un conjunto ordenado parcialmente. Sea el retículo $(A, \cup, \cap)$. Sobre él se establece la relación Ω siguiente:

$$a \in A,\ b \in A,\ a\,\Omega\,b \Leftrightarrow (a \cup b = b) \wedge (a \cap b = a)$$

Para que el teorema quede establecido, habrá de demostrarse que Ω es una relación de orden parcial sobre A. En efecto:

1.º Ω es reflexiva

Según T_2, $\quad (a \cup a = a) \wedge (a \cap a = a) \Leftrightarrow a\,\Omega\,a$

2.º Ω es antisimétrica

$$\left.\begin{array}{l} a\,\Omega\,b \Rightarrow (a \cup b) \wedge (a \cap b = a) \\ b\,\Omega\,a \Rightarrow (b \cup a = a) \wedge (b \cap a = b) \end{array}\right\} \Rightarrow a \equiv b$$

Se ha aplicado la ley A_4.

3.º Ω es transitiva

$$\begin{array}{l} a\,\Omega\,b \Rightarrow (a \cup b = b) \wedge (a \cap b = a) \\ b\,\Omega\,c \Rightarrow (b \cup c = c) \wedge (b \cap c = b) \end{array}$$

Usando la ley T_3 y las hipótesis establecidas, se escribe:

$$\left.\begin{array}{l} a \cup c = a \cup (b \cup c) = (a \cup b) \cup c = b \cup c = c \\ a \cap c = (a \cap b) \cap c = a \cap (b \cap c) = a \cap b = a \end{array}\right\} \Rightarrow a\,\Omega\,c$$

Ejemplo 1

Desarróllese el teorema sobre el álgebra de conjuntos, resaltando la inclusión como la relación de orden que ordena el retículo.

Ejemplo 2

Compruébese que la implicación lógica es la relación que ordena el retículo de las proposiciones.

NOTA. El orden (A, Ω) sobre el retículo A es un orden, en general, parcial, puesto que no todo elemento a y b del retículo cumple que $a \cup b = b$ y $a \cap b = b$, hipótesis establecidas en el teorema.

1.3472. TEOREMA *«recíproco»*

Se ha entrecomillado «recíproco» porque no existe tal teorema. Se quiere decir que la proposición recíproca de la anterior, que dictaría

«todo conjunto parcialmente ordenado es un retículo»

es falsa. Efectivamente, definamos la unión e intersección, en función de la relación de orden, creada *a priori*:

$$(a \cup b = b) \wedge (a \cap b = a) \Leftrightarrow a \,\Omega\, b$$

Como se ve —y ya se advirtió en NOTA—, de este modo quedan definidas las operaciones reticulares, *solamente* para elementos relacionados por Ω. Por tanto, si (A, Ω) fuera un orden total, sí que quedarían definidas en todo su ámbito la reunión e intersección; y en ese caso, se puede escribir:

Todo conjunto totalmente ordenado es un retículo.

Sin embargo, abundando un poco más en la cuestión, si se intentan crear dos operaciones reticulares más restringidas que las generalizadas (la unión e intersección de conjuntos —por ejemplo—), tal vez se consiga hacer compatible el orden parcial con la estructura de retículo que nos proponemos crear.

Sea (A, Ω) un orden parcial, tal que $\forall a \in A$, $\forall b \in A$, cada uno de los subconjuntos $\{a, b\}$ tiene supremo e ínfimo.

Se establecen sobre A las operaciones

$$a \cup b = \sup\{a, b\}$$
$$a \cap b = \inf\{a, b\}$$

Pues bien, tales operaciones son compatibles con la relación de orden parcial Ω; y, *respecto de ellas*, se puede asegurar que

Todo conjunto parcialmente ordenado es un retículo*.

1.348. Buena ordenación

1.3481. *Conjunto bien ordenado*

Sea el orden total (A, Ω). Se dice que A está bien ordenado, mediante Ω, o que (A, Ω) es buena ordenación, si todo subconjunto de A, ordenado con Ω, tiene mínimo (primer elemento). O sea:

$$\left.\begin{array}{l}\text{El orden total } (A, \Omega)\\ \text{es buena ordenación}\end{array}\right\} \Leftrightarrow \forall B \subset A,\ \exists a \in B / a\,\Omega\, x,\ \forall x \in B$$

* Ponemos en guardia al lector respecto de la frecuente e ilógica postura del estudiante superficial. Una lectura «rápida», «a salto de negrita», llevaría al craso error de considerar el recuadro fuera de contexto, adquiriendo, de este modo, un concepto falso.

Ejemplo 1

El orden $(N, \leq)$ es buena ordenación, pues todo subconjunto de los naturales tiene mínimo, respecto de la relación de orden $\leq$.

Ejemplo 2

El orden $(Z, \leq)$ no es buena ordenación, ya que —por ejemplo— el subconjunto ordenado $(Z^-, \leq)$ de los enteros negativos no tiene primer elemento.

1.3482. TEOREMA. Toda buena ordenación es un orden total.

En efecto, si (A, Ω) es un conjunto bien ordenado, todos y cada uno de sus subconjuntos binarios han de tener primer elemento; o sea:

$$\forall\{a, b\} \subset A \Rightarrow (a\,\Omega\,b) \vee (b\,\Omega\,a),$$

que no es más que la condición para que el orden (A, Ω) sea total.

Sin embargo, la proposición recíproca no es cierta. Un contraejemplo zanja la cuestión. Considérese el orden de los racionales con la relación $\leq$. Un subconjunto suyo es —por ejemplo— el conjunto de los racionales negativos, $\{Q^-\}$, que, obviamente, no tiene mínimo en el orden $(Q^-, \leq)$: dado un racional negativo cualquiera, siempre se puede establecer uno menor.

Ejercicio. Demuéstrese el teorema inmediato que dice: «Todo subconjunto de un conjunto bien ordenado es bien ordenado.»

1.3483. *Axioma de elección. Postulado de Zermelo*

Existen tres proposiciones que son equivalentes:

1. *Lema de Zorn*: Todo conjunto inductivo admite, al menos, un elemento maximal.

Dado el conjunto ordenado $(A, \leq)$, se dice que es inductivo, si todo subconjunto totalmente ordenado tiene un mayorante.

2. *Postulado de Zermelo*: Todo conjunto admite una buena ordenación.

Un conjunto ordenado $(A, \leq)$ se dice que está bien ordenado o que admite una buena ordenación, cuando todo subconjunto suyo tiene elemento mínimo.

3. *Axioma de elección*: Dado un conjunto $A \neq \phi$, existe una aplicación

$$\{P(A) - \phi\} \xrightarrow{f} B,$$

tal que a todo $B \subset A$ hace corresponder un elemento $f(B) \in B$.

Se demuestra mediante un proceso largo, pero no difícil, que las tres proposiciones anteriores son equivalentes. La demostración se realiza mediante la implicación

Lema de Zorn ⇒ Postulado de Zermelo ⇒ Axioma de elección ⇒ Lema de Zorn.

No la desarrollaremos porque rebasa ampliamente los límites de este libro.

Adviértase que si se admite una de las proposiciones, por ejemplo, el axioma de elección, que es el más intuitivo, los otros dos pueden considerarse teoremas. El llamado «Teorema de la buena ordenación» es precisamente el postulado de Zermelo, y se demuestra dando por buenos el axioma de elección o el lema de Zorn.

Cualquiera de las tres proposiciones asegura que *todo conjunto admite una buena ordenación.*

1.35. EL ALGEBRA DE LAS RELACIONES

Definida una relación binaria, tal como se hizo en 1.321, como una proposición lógica sobre un subconjunto de un cartesiano, que es su conjunto de validez, de un modo natural, cabe construir un álgebra de relaciones, siguiendo paso a paso el álgebra de las proposiciones*.

En primer lugar, habrán de establecerse las relaciones de igualdad y orden que se correspondan con las de equivalencia lógica e implicación lógica del álgebra de proposiciones (las de igualdad de conjuntos e inclusión, del álgebra conjuntista).

Luego se crearán dos operaciones binarias entre relaciones, equivalentes a la disyunción y conjunción lógicas (unión e intersección de conjuntos) y otra unitaria, análoga a la negación de proposiciones (la complementación de conjuntos).

Finalmente, se resaltará que el conjunto de las relaciones, así estructurado, por cumplir las leyes que repetidamente se han venido estableciendo, constituye un álgebra de Boole (es decir, un retículo complementario distributivo, como se verá en el capítulo 2.1).

1.351. Igualdad y orden en el conjunto de las relaciones

Dos relaciones sobre el conjunto A, S y T son iguales si su grafo es el mismo; lo que quiere decir que su conjunto de validez, $A^2_{[1]}$, es el mismo subconjunto del cartesiano $A \times A$; y esto solamente sucederá si el enunciado p y el enunciado q, sobre A^2, producen dos proposiciones lógicamente equivalentes.

---

* Pudiera preferirse seguir la construcción a partir del álgebra de conjuntos; no en balde, una relación queda fijada con un subconjunto del conjunto cartesiano sobre el que se define: su conjunto de validez. La descripción sería distinta, pero la realidad matemática la misma y, por supuesto, se llegaría a la misma meta.

Ejemplo

Sea $A = \{2, 4, 8, 16\}$ y sobre él las relaciones S = «ser menor o igual que» y T = «ser divisor de».

Con los símbolos que se vienen utilizando,

$$S = (A^2_{[1]}, \leq) \quad ; \quad T = (A^2_{[1]}, x/y)$$

El grafo de S es

$$G(S) = \{(2, 2), (2, 4), (2, 8), (2, 16), (4, 4), (4, 8), (4, 16), (8, 8), (8, 16), (16, 16)\}$$

Compruébese que el de T es el mismo.

Luego nos encontramos frente a dos relaciones iguales y, en efecto, las proposiciones relacionales son lógicamente equivalentes.

La posible extrañeza frente a la última frase escrita puede surgir de un error de interpretación: «¿cómo es posible que se pueda establecer que $\leq \Leftrightarrow x/y$?

La pregunta no procede de una madura reflexión. «Ser menor que» o «ser divisor de» NO son proposiciones, sino simples enunciados que, en lo que no se refieran a los elementos del cartesiano sobre los que se establecen, no tienen valor de verdad alguno: no son proposiciones. Lo que sí es cierto es que las proposiciones que se escriben son lógicamente equivalentes. Analícese

$$(A^2_{[1]}, \leq) \Leftrightarrow (A^2_{[1]}, x/y)$$

Por lo que se refiere a establecer un orden sobre el conjunto de las relaciones, es claro que la implicación lógica de sus proposiciones asociadas exige la inclusión de los conjuntos de validez de las mismas.

Diremos entonces que la relación S implica la T o que la relación S está incluida en la T, si la proposición de S implica la proposición de T, o si el conjunto de validez de S es subconjunto del conjunto de validez de T.

Ejemplo

Sobre el conjunto de los naturales se establecen las relaciones $S = (N^2_{[1]}, >)$ y $T = (N^2_{[1]}, \neq)$.

La relación $S \subset T$, ya que

$$a \in N,\ b \in N,\ a > b \Rightarrow a \neq b$$

1.352. Operaciones con relaciones

1.3521. *Unión o disyunción de relaciones*

Sea la relación S sobre A, cuyo conjunto de validez es el subconjunto $M \subset A^2$; y sea la T, que es cierta sobre $N \subset A^2$.

$$S = (M, p) \quad ; \quad T = (N, q)$$

Definimos una relación F sobre A, cuyo enunciado proposicional es la disyunción lógica de p y q:

$$F = (A^2_{[1]},\ p \vee q)$$

¿Cuál es el conjunto de validez de F? Es obvio que F resulta cierta para el conjunto-unión de los de validez de S y T, de modo que

$$F = (M \cup N,\ p \vee q)$$

La relación F así creada es la relación-reunión de las S y T. Denotamos

$$F = S \cup T$$

Ejemplo

Sobre el conjunto $A = \{1, 2, 3, 4\}$ se establece la relación $S =$ «ser igual que» y también la $T =$ «ser menor que».

Los conjuntos de validez o grafos de ambas son:

$$A^2_S = \{(1, 1),\ (2, 2),\ (3, 3),\ (4, 4)\}$$
$$A^2_T = \{(1, 2),\ (1, 3),\ (1, 4),\ (2, 3),\ (2, 4),\ (3, 4)\}$$

Sea ahora, sobre A, la relación $F =$ «ser menor o igual que». Su conjunto de validez, obviamente, es:

$$A^2_F = A^2_S \cup A^2_T$$

La relación F es la unión de S y T

$$(A^2_{[1]},\ \leq) = (A^2_{[1]},\ <) \cup (A^2_{[1]},\ =)$$

1.3522. *Intersección o conjunción de relaciones*

Con idénticos términos de planteamiento que los del número anterior, definimos una relación Y, cuyo enunciado proposicional es la conjunción lógica de p y q:

$$Y = (A^2_{[1]},\ p \wedge q)$$

El conjunto de validez de Y es la intersección de los grafos de S y T. Resulta entonces, que

$$Y = (M \cap N,\ p \wedge q)$$

Esta relación Y es la intersección de las relaciones S y T; denotamos

$$Y = S \cap T$$

Ejemplo

Sobre el conjunto de cuadros, C, de una exposición de pintura contemporánea, se establecen las relaciones S = «ser del mismo autor» y T = «pertenecer a la misma época». Así, siendo $M \subset C^2$, el conjunto de validez de S y $N \subset C^2$, el de T, todo par del conjunto $M \cap N$ estará formado por dos cuadros con la misma firma y pintados en la misma época. Por ejemplo, eso sucederá con *Los tres músicos* y *Mandolina y guitarra*, ambos, lienzos de Picasso, pintados, el uno, en 1921, el otro en 1924, encuadrados los dos en su etapa de «cubismo evolucionado».

1.3523. *Relaciones complementarias o negación de relaciones*

Sea la relación $R = (A^2_{[1]}, p)$.

Entendamos, para mayor comodidad tipográfica, que su conjunto de validez es M; o sea $A^2_{[1]} \equiv M$.

La relación cuyo enunciado proposicional sea $\sim p$ tendrá el conjunto de validez N, de tal manera que

$$M \cup N = A^2$$

y

$$M \cap N = \phi,$$

lo cual define a N como el complementario de M en A^2.

Efectivamente, definiremos una operación unitaria sobre el conjunto de las relaciones, que llamaremos complementación, de la siguiente manera:

$\bar{R}$ es relación complementaria de la $R = (A^2_{[1]}, p)$, si

$$\bar{R} = ((A^2_{[1]})', \sim p)$$

Ejemplo

Sea la relación R = «ser divisor de» sobre el conjunto $A = \{2, 3, 6, 8\}$.

Su grafo o conjunto de validez es

$$M = \{(2, 2), (2, 6), (2, 8), (3, 3), (3, 6), (6, 6), (8, 8)\}$$

La relación $\bar{R}$ = «no ser divisor de» sobre A tiene por conjunto de validez el complementario de M en A^2; a saber:

$$N \equiv M' = \{(2, 3), (3, 2), (3, 8), (6, 2), (6, 3), (6, 8), (8, 2), (8, 3), (8, 6)\}$$

1.353. El álgebra de las relaciones

Una vez más nos encontramos frente a otra concreción de la misma estructura algebraica.

El conjunto de las relaciones, con las operaciones establecidas, responde a idéntica estructura que el de los conjuntos y el de las proposiciones; son distintas descripciones de la misma estructura matemática: el álgebra de Boole.

Todas y cada una de las leyes que se han establecido en los capítulos anteriores, para este álgebra, son válidas aquí.

1.354. Producto de relaciones

Considérese la relación S entre los elementos del conjunto A y los del conjunto B. Y también, establezcamos una relación T entre los elementos de B y los de un tercer conjunto C*.

Supóngase que existen un $a \in A$ y un $b \in B$, para los que la relación S es cierta:

$$a\, S\, b$$

y que hay un $c \in C$, de modo que

$$b\, T\, c$$

Se crea una nueva relación, que llamaremos *producto de relaciones* entre los elementos de A y de C, en la que a y c están relacionados:

$$a\, (S \times T)\, c$$

Ejemplo

Sea A el conjunto de todos los pintores contemporáneos (entiéndase «del todo» definido) y sea B el de las obras pictóricas modernas catalogadas (también perfectamente determinadas). La relación S = «fue pintado por» actúa sobre el cartesiano $A \times B$, de modo que el par

(Picasso, *Los tres músicos*) pertenece a S; y el
(Gris, *Tablero de ajedrez*) también; pero el
(Gris, *Arlequín*) no es de su conjunto de validez; y el
(Léger, *La musa*), tampoco.

Sea ahora C el conjunto de todas las pinacotecas (museos y colecciones particulares) y T la relación «encontrarse en», definida sobre el cartesiano $B \times C$, de modo que el par

(*Los tres músicos*, Nueva York) es par de T; y
(*Tablero de ajedrez*, Chicago), también.

El par (Picasso, Nueva York), creado «a través» de su tela *Los tres músicos*, pertenece a la relación $S \times T$ = «tiene obras en», cuyo conjunto de validez es subconjunto del cartesiano $A \times C$.

---

* Se prefieren utilizar aquí diversos conjuntos en lugar de uno solo, a fin de resaltar claramente los conceptos que se desean establecer.

1.36. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

1.360.
Justifíquese que la relación complementaria de $(N^2_{[1]}, >)$ es $(N^2_{[1]}, \leq)$.

1.361.
Demuéstrese que la relación recíproca del producto $S \times T$ coincide con el producto de las recíprocas, cambiadas de orden, $T^{-1} \times S^{-1}$.

1.362.
El producto de relaciones es asociativo. Justifíquese.

1.363.
Establézcanse y analícense todos los órdenes que la relación $\leq$ produce sobre los conjuntos N, Z, Q, R y C.

1.364.
Sea P el conjunto de todos los polígonos regulares convexos de igual radio y centro, con un vértice común en A.

Se define una relación Ω, sobre P, de modo que $P_1 \,\Omega\, P_2$, simboliza que los vértices de P_1 coinciden con vértices de P_2.

a) Justifíquese que Ω es una relación de orden sobre P.
b) Analícese si se trata de un orden total o parcial.
c) Estúdiese la posibilidad de que (P, Ω) sea una buena ordenación.

1.365.
Sobre el mismo conjunto P del número anterior, se establece ahora una relación ω, del siguiente modo

$$P_1 \in P,\ P_2 \in P,\ P_1\ \omega\ P_2 \Leftrightarrow l_1 \leq l_2,$$

donde l_1 y l_2 son los lados de los polígonos P_1 y P_2.

a) Justifíquese que (P, ω) es un orden total.
b) Analícese si (P, ω) es buena ordenación.

1.366.
Establézcase el concepto de número cardinal, mediante la relación de coordinabilidad sobre el conjunto $P(U)$ de los conjuntos.

1.367.
Entiéndase por N el conjunto de los naturales con el cero.

Sea la relación R, definida sobre N^2 de este modo:

$$(a, b) \in N^2,\ (c, d) \in N^2,\ (a, b)\ R\ (c, d) \Leftrightarrow a + d = c + b$$

a) Demuéstrese que se trata de una relación de equivalencia.
b) Muéstrese la acción de R sobre N^2.
c) Establézcase el conjunto-cociente N^2/R, que es el conjunto de los números enteros, Z.

d) Escójase para las clases enteras sus representantes canónicos.

1.368.

Denotamos por $Z^0 = Z - \{0\}$. Sobre $Z \times Z^0$ se crea la relación R, definida de este modo:

$$(a, b) \in Z \times Z^0,\ (c, d) \in Z \times Z^0,\ (a, b)\, R\, (c, d) \Leftrightarrow a \cdot d = c \cdot b$$

a) Pruébese que se trata de una relación de equivalencia.

b) Muéstrese la acción de R sobre $Z \times Z^0$.

c) Establézcase el conjunto-cociente, $Z \times Z^0/R$, que es el conjunto de los números racionales, Q.

d) Escójanse para las clases racionales sus representantes canónicos.

1.369.

Justifíquese que el orden $(Q, \leq)$ es un «orden denso», en el sentido de que entre dos racionales cualesquiera siempre puede introducirse otro, comprendido entre los datos.

2

ALGEBRA BASICA

BIBLIOGRAFIA 2

D. KAYE: *Sistemas booleanos*. Ed. Alhambra. Madrid, 1970.

A. LENTIN y J. RIVAUD: *Algebra Moderna*. 2.ª ed., 1.ª reimp. Ed. Aguilar. Madrid, 1969.

GODEMENT: *Algebra*. Ed. Tecnos. Madrid, 1971.

C. PISOT y M. ZAMANSKY: *Matemáticas Generales*. Ed. Montaner y Simón. Barcelona, 1970.

O. ZARISKI y P. SAMUEL. *Comutative Algebra* (2 vols.), D. Van Nostrand Co. Inc. Princeton, New Jersey. Colec. «The University Series in Higher Mathematics».

2.1

Algebra de Boole

2.10. Introducción

2.11. Retículos. Retículos complementarios. Algebra de Boole

2.12. Principio de dualidad

2.13. Axiomática de Huntington para un álgebra de Boole

2.14. Axiomática de Birkhoff-McLane para un álgebra de Boole

2.15. Axiomática de Stoll-Goodstein para un álgebra de Boole

2.16. Teoremática del álgebra de Boole

2.17. El álgebra de Boole del «todo o nada»

2.18. Funciones booleanas

2.19. Aplicabilidad. Automatismos y destrezas

2.1

Algebra de Boole

2.10. INTRODUCCION

Descrito el modelo que subyace en toda la Matemática, al desarrollar la Teoría de Conjuntos de Cantor en los capítulos que anteceden, ahora se pretende dar el segundo paso del trabajo matemático: crear estructuras.

Se habrá observado el idéntico comportamiento de las proposiciones con sus conectivas lógicas $\vee$, $\wedge$ y $\sim$, y el de los conjuntos, con sus leyes de $\cup$, $\cap$ y $'$. Otros modelos, como los espacios probabilísticos de sucesos estocásticos o los circuitos eléctricos de interruptores absolutos, más adelante nos sorprenderán con igual comportamiento.

Todo ello obliga a abstraer y, desnudando de sus concreciones a los sistemas citados, concebir un modelo matemático, abstracto que, vacío de todo contenido específico, sea sin embargo válido para llenarlo en cada ocasión con los dispares sistemas concretos que lo sugirieron.

Resulta así, como un «molde legislativo», dispuesto a producir, en cualquier momento «manufacturados matemáticos» con los materiales positivos que el mundo de la materia-energía suministre.

Este «molde», esta primera estructura que nos disponemos a crear, es el álgebra de Boole.

Al construir un sistema axiomático, el matemático es libre de establecer sus axiomas, con tal de que resulte un conjunto axiomático suficiente, independiente y compatible (véase página 28; de ahí que puedan surgir diferentes axiomáticas, equivalentes entre sí, ya que lo que un autor postula como axioma, otro puede considerarlo como teorema, si —a su vez— una proposición que era teoremática para el primero, el segundo lo establece como axioma. Así resulta en el caso que nos ocupa: citaremos nosotros cuatro sistemas axiomáticos distintos para el ál-

gebra de Boole, que habrá de probarse que son equivalentes. Y ello, no por el afán de un coleccionismo enciclopédico, fuera de lugar —del todo— en este libro, sino porque consideramos sumamente formativo el estudio comparado sobre autores distintos, uno de los modos ineludibles de abordar el aprendizaje científico. Trataremos, pues, las axiomáticas «reticular»*, de Huntington, de Birkhoff-McLane y de Stoll-Goodstein.

Inmediatamente antes de iniciar el estudio, nos queda decir que no hemos seguido el orden tradicional en la exposición de axiomas con el fin de que el estudio comparado al que antes aludíamos no produzca engorrosos solapamientos intermedios.

2.11. RETICULOS. RETICULOS COMPLEMENTARIOS. ALGEBRA DE BOOLE

Sea un conjunto $A = \{a, b, c, \ldots, z\}$ y dos operaciones entre sus elementos que denotaremos genéricamente por $*$ y $\perp$.

Diremos que la terna $[A, *, \perp]$ es un retículo, si, respecto de las dos operaciones, se dan las cuatro leyes de Absorción, Idempotencia, Asociatividad y Conmutatividad.

Explicitemos:

$[A, *, \perp]$ *es RETICULO*

A_1)	*Absorción*	
	$a * (a \perp b) = a$	$a \perp (a * b) = a$
A_2)	*Idempotencia*	
	$a * a = a$	$a \perp a = a$
A_3)	*Asociatividad*	
	$a * (b * c) = (a * b) * c$	$a \perp (b \perp c) = (a \perp b) \perp c$
A_4)	*Conmutatividad*	
	$a * b = b * a$	$a \perp b = b \perp a$

* Excúsesenos la pequeña osadía de poner nombre determinativo al modo tradicionalmente elemental de presentar la axiomática del álgebra de Boole. En nuestra intencionalidad didáctica, necesitábamos un nombre, y tal vez ése no resulte desafortunado en exceso.

El nombre de «retículo» procede de que al intentar dibujar un esquema del conjunto A, estructurado de este modo y dotado de un orden parcial Ω, aparece una red cúbica que evoca una distribución cristalina iónica.

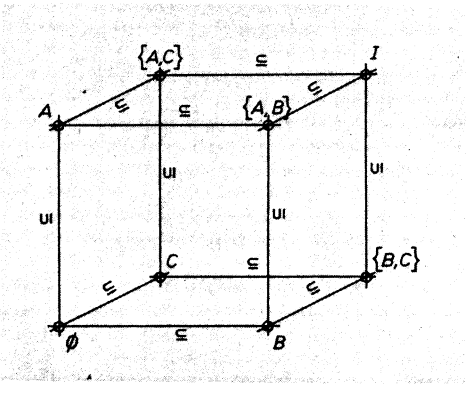
Ejemplo 1

El conjunto de todos los conjuntos $\mathcal{P}(C)$ con la relación de inclusión $\subseteq$, y sus operaciones de reunión $\cup$ e intersección $\cap$, forma un retículo en el que los nudos de la red vienen ocupados por los conjuntos (elementos de $\mathcal{P}(C)$), ordenados parcialmente por la relación de inclusión.

Sea la célula $\mathcal{P}(I)$, siendo $I = \{A, B, C\}$

$$\mathcal{P}(I) = \{\phi, \{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}.$$

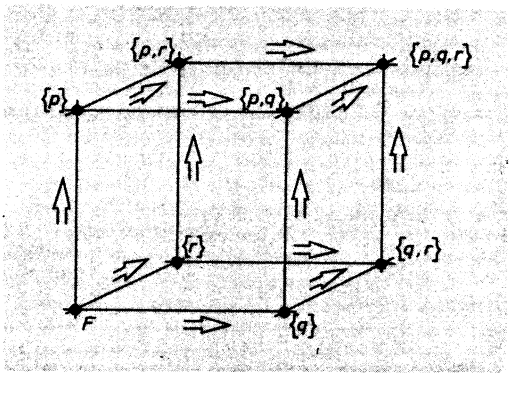
Su representación es:



Ejemplo 2

El conjunto de las proposiciones $\mathcal{P}(P)$, con la relación de implicación lógica $\Rightarrow$, y sus operaciones de disyunción $\vee$, y conjunción $\wedge$ forma un retículo.

Sea $P = \{p, q, r\}$ y $\mathcal{P}(P) = \{F, \{p\}, \{q\}, \{r\}, \{p, q\}, \{p, r\}, \{q, r\}, \{p, q, r\}\}$.



Establezcamos ahora sobre A una operación unitaria, que llamaremos *complementación* y signaremos por un apóstrofe junto al operando; de este modo:

$$a' = b \Leftrightarrow (a * b = A) \wedge (a \perp b = \phi)$$

Ello constituye un quinto axioma, llamado de complementariedad

A_5) *Complementariedad*	
$a * a' = U$	$a \perp a' = \phi$

Los cinco axiomas precedentes suministran a $[A, *, \perp]$ la estructura de *retículo complementario.*

La complementariedad en el álgebra de conjuntos toma la forma, ya vista, de

$$A \cup A' = U \quad ; \quad A \cap A' = \phi$$

En el álgebra proposicional recibe el nombre específico de negación, y, siendo el universal la tautología V y el vacío la contradicción F, la escritura es

$$p \vee (\sim p) = V \quad ; \quad p \wedge (\sim p) = F$$

Obliguemos, además, a que se cumpla una sexta ley:

A_6) *Distributividad*	
$a * (b \perp c) = (a * b) \perp (a * c)$	$a \perp (b * c) = (a \perp b) * (a \perp c)$

Alcanzamos así para $[A, *, \perp]$ una estructura de retículo complementario distributivo, por otro nombre, *álgebra de Boole.*

Tanto el conjunto de los conjuntos como el de las proposiciones que venimos intercalando son álgebras de Boole, tal y como quedó establecido en sus correspondientes desarrollos monográficos.

De modo que conjuntando lo dicho, sinópticamente, resulta el siguiente cuadro:

A_1) Absorción * y $\perp$	*Retículo*	*Retículo complementario*	*Algebra de Boole*
A_2) Idempotencia * y $\perp$			
A_3) Asociatividad * y $\perp$			
A_4) Conmutatividad * y $\perp$			
A_5) Complementariedad			
A_6) Distributividad * y $\perp$			

2.12. PRINCIPIO DE DUALIDAD

En la recién establecida álgebra de Boole se habrá observado que la axiomática se ha construido a dos columnas, referibles a cada una de las operaciones binarias; y que bastaría sustituir en los enunciados de la primera columna el signo $*$ por el signo $\perp$, para obtener los de la segunda.

Aparte de lo dicho, considérense los elementos extremos del orden Ω, que se refieren al universal y al vacío. Pues bien: se denomina enunciado dual de otro al que resulta de intercambiar los signos $*$, $\perp$ y los elementos extremos ϕ y $\cup$.

El principio de dualidad dicta: «En toda estructura en que coexistan dos axiomas duales, sucede que todo teorema deducido de uno de ellos implica su teorema dual.»

Usaremos continuamente de este principio en los desarrollos algebraicos que siguen.

2.13. AXIOMATICA DE HUNTINGTON PARA UN ALGEBRA DE BOOLE

Tal vez sea éste el sistema axiomático más simple para esta estructura.

Huntington postula para su álgebra de Boole tres axiomas coincidentes con el sistema anterior, que son:

A_4) Conmutatividad $*$ y $\perp$,
A_5) Complementariedad,
A_6) Distributividad $*$ y $\perp$,

e introduce uno nuevo, que numeraremos séptimo, y que es

A_7) *Identidad*	
$a * \phi = a$	$a \perp U = a$

En el conjunto de los conjuntos toma la forma

$$A \cup \phi = A \quad ; \quad A \cap U = A;$$

en el de las proposiciones

$$p \vee F = p \quad ; \quad p \wedge V = p$$

Para justificar que nos encontramos frente a dos axiomáticas equivalentes, habrán de demostrarse dos cosas:

a) que los axiomas A_1, A_2 y A_3 se pueden deducir de los A_4, A_5, A_6 y A_7 de Huntington;
b) que el axioma A_7 de Huntington es deducible a partir de los seis primeros del primer sistema.

Procedamos, pues, a la justificación.

a-1) *Absorción* (A_1)
Teorema previo: $(a * U = U) \wedge (a \perp \phi = \phi)$
En efecto:

$$\begin{aligned} a * U &= U \perp (a * U) && \text{según los axiomas } A_7 \text{ y } A_4 \\ &= (a * a') \perp (a * U) && \text{según } A_5 \\ &= a * (a' \perp U) && \text{según } A_6 \\ &= a * a' && \text{según } A_7 \\ &= U && \text{según } A_5, \text{ c.q.d.} \end{aligned}$$

Demuéstrese, como ejercicio, de manera análoga el teorema dual.
Con este teorema demostrado, ya podemos pasar a probar la ley de absorción

$$\begin{aligned} a * (a \perp b) &= (a \perp U) * (a \perp b) && \text{según } A_7 \\ &= a \perp (U * b) && \text{según } A_6 \\ &= a \perp U && \text{en razón del teorema previo} \\ &= a && \text{según } A_7, \text{ c.q.d.} \end{aligned}$$

Realícese el ejercicio de justificar de manera análoga el enunciado dual.

a-2) *Idempotencia* (A_2)

$$\begin{aligned} a * a &= (a * a) \perp U && \text{según } A_7 \\ &= (a * a) \perp (a * a') && \text{según } A_5 \\ &= a * (a \perp a') && \text{según } A_6 \\ &= a * \phi && \text{según } A_5 \\ &= a && \text{según } A_7, \text{ c.q.d.} \end{aligned}$$

Puede establecerse el dual $a \perp a = a$, bien mediante una deducción similar, bien aplicando el principio de dualidad.

a-3) *Asociatividad* (A_3)
La recién probada ley de absorción nos permite escribir esta identidad

$$\begin{aligned} a \perp [a * (b * c)] &= a && \text{según } A_1 \\ &= a * (a \perp c) && \text{según } A_1 \\ &= [a \perp (a * b)] * (a \perp c) && , \text{ también por } A_1 \\ &= a \perp [(a * b) * c] && \text{según } A_6 \end{aligned}$$

Hemos conseguido así la identidad

$$a \perp [a * (b * c)] = a \perp [(a * b) * c] \qquad [1]$$

Ahora, el axioma de distributividad, A_6, permite establecer esta identidad

$$\begin{aligned}
a' \perp [a * (b * c)] &= (a' \perp a) * [a' \perp (b * c)] && \text{según } A_6 \\
&= \phi * [a' \perp (b * c)] && \text{según } A_5 \\
&= a' \perp (b * c) && \text{según } A_7 \\
&= (a' \perp b) * (a' \perp c) && \text{según } A_6 \\
&= [\phi * (a' \perp b)] * (a' \perp c) && \text{según } A_7 \\
&= [(a' \perp a) * (a' \perp b) * (a' \perp c) && \text{según } A_5 \\
&= [a' \perp (a * b)] * (a' \perp c) && \text{según } A_6 \\
&= a' \perp [(a * b) * c] && \text{según } A_6
\end{aligned}$$

Hemos llegado a establecer la identidad

$$a' \perp [a * (b * c)] = a' \perp [(a * b) * c] \qquad [2]$$

Componiendo miembro a miembro las igualdades [1] y [2] con $*$, resulta:

$$[a \perp (a * (b * c))] * [a' \perp (a * (b * c))] = [a \perp ((a * b) * c)] * [a' \perp ((a * b) * c)]$$

aplicando $A_4 \Downarrow$

$$[(a * (b * c)) \perp a] * [(a * (b * c)) \perp a'] = [((a * b) * c) \perp a] * [((a * b) * c) \perp a']$$

aplicando $A_6 \Downarrow$

$$[a * (b * c)] \perp (a * a') = [(a * b) * c] \perp (a * a')$$

$\Downarrow$ en virtud de A_5

$$[a * (b * c)] \perp U = [(a * b) * c] \perp U$$

$\Downarrow$ en razón de A_7

$$a * (b * c) = (a * b) * c$$

Similar desarrollo o la aplicación del principio de dualidad permiten justificar la asociatividad para la operación $\perp$.

b) *Identidad* (A_7)

Toca ahora probar que el axioma de identidad de Huntington

$$(A_7) \begin{cases} a * \phi = a \\ a \perp U = a \end{cases}$$

es deducible como teorema, a partir de los seis postulados de la axiomática reticular,

En efecto:

$$\begin{aligned}
a * \phi &= a * (a \perp a'), && \text{por complementariedad } (A_5); \\
&= a \quad , && \text{por idempotencia } (A_1).
\end{aligned}$$

De igual modo, la proposición dual

$$\begin{aligned}
a \perp U &= a \perp (a * a'), && \text{por complementariedad } (A_5); \\
&= a \quad , && \text{por idempotencia } (A_1).
\end{aligned}$$

Claro es que la aplicación del Principio de Identidad hubiera ahorrado el segundo desarrollo.

Ejercicios

1. ¿Qué formas tomarían estas demostraciones en álgebra proposicional?
2. Justificar la ley A_7, partiendo de la identidad $a * \phi = a \perp U$.

Como se pretendía, queda demostrado que ambas axiomáticas, la «reticular» y la de Huntington, son equivalentes. Bueno será esquematizar la situación sinópticamente:

Axiomática «reticular»	A_1) Absorción * y $\perp$	
	A_2) Idempotencia * y $\perp$	
	A_3) Asociatividad * y $\perp$	
	A_4) Conmutatividad * y $\perp$	Axiomática de Huntington
	A_5) Complementariedad	
	A_6) Distributividad * y $\perp$	
	A_7) Identidad * y $\perp$	

2.14. AXIOMATICA DE BIRKHOFF-MCLANE PARA UN ALGEBRA DE BOOLE

Este sistema de axiomas utiliza como tales seis de las siete leyes que venimos estableciendo, prescindiendo de la absorción; además, establece las siguientes, que numeramos correlativamente:

A_8) *Involución*

$$(a')' = a$$

A_9) *Igualdad de De Morgan*

$$(a * b)' = a' \perp b' \qquad (a \perp b)' = a' * b'$$

A_{10}) *Existe en* $[A, *, \perp]$ *una relación de orden parcial* Ω

A_{11}) *Los extremos absolutos del orden* $[A, \Omega]$ *existen, denotados por* ϕ *y* U

a) La igualdad de De Morgan toma la forma

$$(A \cup B)' = A' \cap B' \quad ; \quad (A \cap B)' = A' \cup B',$$

para el conjunto de los conjuntos; mientras que en el álgebra proposicional es

$$\sim(p \vee q) = \sim p \wedge \sim q \quad ; \quad \sim(p \wedge q) = \sim p \vee \sim q$$

b) La involución es

$$(A')' = A;$$

y con proposiciones

$$\sim(\sim p) = p$$

c) La relación de orden de A_{10} es la relación de inclusión entre conjuntos, $\subseteq$; mientras que la relación de orden proposicional es la implicación $\Rightarrow$.

d) Los extremos absolutos para conjuntos son el conjunto vacío y el universal; para el conjunto de las proposiciones son, respectivamente, la contradicción F y la tautología V.

Manteniendo nuestra línea de consistencia lógica en la exposición, ahora habría de comprobarse que el sistema de axiomas establecido es equivalente a uno de los otros dos descritos, por ejemplo, el de Huntington.

Advirtiendo que la relación de orden que postulan Birkhoff y McLane tiene en las otras axiomáticas la equivalencia que se describe, dejamos al interés o conveniencia del lector realizar esta tarea, muy provechosa, si lo que intenta es andar con soltura en estos modos estructurales.

$$a \,\Omega\, b \Leftrightarrow (a \perp b = a) \wedge (a * b = b) \qquad [1]$$

Es intuitiva esa relación abstracta en el álgebra de conjuntos. Su traducción en términos conjuntistas es

$$A \subseteq B \Leftrightarrow A \cap B = A;$$

si de proposiciones se trata, se escribe:

$$p \Rightarrow q \Leftrightarrow p \wedge q = p$$

Un nuevo cuadro sinóptico incorpora la axiomática, recientemente descrita:

Axiomática «reticular»	A_1)	Absorción * y $\perp$		Axiomática Birkhoff-McLane
	A_2)	Idempotencia * y $\perp$		
	A_3)	Asociatividad * y $\perp$		
	A_4)	Conmutatividad * y $\perp$	Axiomática de Huntington	
	A_5)	Complementariedad		
	A_6)	Distributividad * y $\perp$		
	A_7)	Identidad * y $\perp$		
	A_8)	Involución		
	A_9)	Igualdad de De Morgan * y $\perp$		
	A_{10})	Relación de orden parcial, Ω		
	A_{11})	Extremos absolutos de Ω: ϕ y U		

2.15. AXIOMATICA DE STOLL-GOODSTEIN PARA UN ALGEBRA DE BOOLE

Este cuarto sistema de axiomas construye un álgebra de Boole usando solamente una operación binaria (la que venimos denotando $\perp$) y la unitaria de la complementación.

Así, al conjunto $[A, \perp, \urcorner]$ le exige tres axiomas, que son:

estos dos, ya establecidos con amplitud dual:

Ab_3) Asociatividad $\perp$
Ab_4) Conmutatividad $\perp$;

y este nuevo, doble:

$$A_{12}) \quad \forall a \in A, \quad \forall b \in A, \quad \forall c \in A \qquad a \perp b' = c \perp c' \Leftrightarrow a \perp b = a$$

Justificar la consistencia de esta axiomática con las tres anteriores, exige crear la operación $*$ con elementos de aquélla. Es de este modo:

$$a * b = (a' \perp b')'$$

Con la noticia anterior, el lector que le apetezca puede intentar —en las dos fases de siempre— justificar la equivalencia del sistema axiomático de Stoll-Goodstein con los tres que le preceden.

2.16. TEOREMATICA DEL ALGEBRA DE BOOLE

Adoptamos la axiomática de Huntington, y en este número, a partir de ella, estableceremos algunos teoremas relevantes del álgebra de Boole.

También recapitularemos aquí los teoremas que han sido desarrollados al justificar la consistencia de las distintas axiomáticas expuestas.

TEOREMA 1

$$(a * U = U) \wedge (a \perp \phi = \phi)$$

Demostrado en a-1).

TEOREMA 2

Ley de absorción:

$$[a * (a \perp b) = a] \wedge [a \perp (a * b) = a]$$

Demostrado en a-1).

TEOREMA 3

Ley de idempotencia:

$$(a * a = a) \wedge (a \perp a = a)$$

Demostrado en *a*-2).

TEOREMA 4

Ley asociativa:

$$[a * (b * c) = (a * b) * c] \wedge [a \perp (b \perp c) = (a \perp b) \perp c]$$

Demostrado en *a*-3).

TEOREMA 5

Todo elemento de un álgebra de Boole tiene complementario único.

Demostración al absurdo: admitamos que a tiene dos complementarios distintos, a'_1 y a'_2; por el axioma de complementariedad (A_5), se establece:

$$a * a'_1 = U; \quad a \perp a'_1 = \phi; \quad a * a'_2 = U; \quad a \perp a'_2 = \phi$$

$a'_1 = a'_1 \perp U$	según A_7
$= a'_1 \perp (a * a'_2)$	según A_5
$= (a'_1 \perp a) * (a'_1 \perp a'_2)$	según A_6
$= \phi * (a'_1 \perp a'_2)$	según A_4 y A_5
$= a'_1 \perp a'_2$	según A_7
$= (a'_1 \perp a'_2) * \phi$	según A_7
$= (a'_1 \perp a'_2) * (a \perp a'_2)$	según A_5
$= (a'_2 \perp a'_1) * (a'_2 \perp a)$	según A_4
$= a'_2 \perp (a'_1 * a)$	según A_6
$= a'_2 \perp U$	según A_5
$= a'_2$	según A_7

TEOREMA 6

El complementario de a' es a; es decir: $(a')' = a$ (Ley de involución).

Sea b un elemento del álgebra de Boole:

Por complementariedad (A_5)

$$b * b' = U \quad ; \quad b \perp b' = \phi \qquad [1]$$

Por conmutatividad (A_4)

$$b' * b = U \quad ; \quad b' \perp b = \phi \qquad [2]$$

Supongamos que $b = a'$; entonces, en [2],

$$(a')' * a' = U \quad ; \quad (a')' \perp a' = \phi \qquad [3]$$

Como el axioma de complementariedad (A_5) ha de cumplirse, sucede que

$$a * a' = U \quad ; \quad a \perp a' = \phi \qquad [4]$$

y si el complementario es único, al comparar [3] y [4], resulta necesariamente que

$$(a')' = a$$

Consecuencia inmediata del teorema es el corolario

$$(\phi = U) \wedge (U' = \phi)$$

(Justifíquese.)

TEOREMA 7

Ley de De Morgan: En toda álgebra de Boole, el complementario del compuesto de dos elementos, mediante una operación, es igual al compuesto de complementarios, mediante la otra; es decir:

$$[(a * b)' = a' \perp b'] \wedge [(a \perp b)' = a' * b']$$

El axioma de distributividad nos permite establecer esta identidad:

$$\begin{aligned}
(a * b) * (a' \perp b') &= (a * b * a') \perp (a * b * b') && \text{según } A_6 \\
&= (a * a' * b) \perp (a * b * b') && \text{según } A_4 \\
&= (U * b) \perp (a * U) && \text{según } T_4 \text{ y } A_5 \\
&= U \perp U && \text{según } T_1 \\
&= U && \text{según } T_3
\end{aligned}$$

Es decir:

$$(a * b) * (a' \perp b') = U \qquad [5]$$

Ahora, el axioma de conmutatividad justifica esta identidad inicial

$$\begin{aligned}
(a * b) \perp (a' \perp b') &= (a' \perp b') \perp (a * b) && \text{según } A_4 \\
&= (a' \perp b' \perp a) * (a' \perp b' \perp b) && \text{según } A_6 \\
&= (a \perp a' \perp b') * (a' \perp b \perp b') && \text{según } A_4 \text{ (dos veces)} \\
&= (\phi \perp b') * (a' \perp \phi) && \text{según } A_5 \\
&= (b' \perp \phi) * (a' \perp \phi) && \text{según } A_4 \\
&= \phi * \phi && \text{según } T_1 \\
&= \phi && \text{según } T_3;
\end{aligned}$$

o sea:

$$(a * b) \perp (a' \perp b') = \phi \qquad [6]$$

La contemplación conjunta de las identidades [5] y [6] induce inmediatamente a establecer el complementario de $(a * b)$; es decir:

$$(a * b)' = a' \perp b', \qquad \text{c.q.d.}$$

Justifíquese, a título de ejercicio, el enunciado dual.

TEOREMA 8

En toda álgebra de Boole existe una relación de orden parcial, Ω.

Habiendo adoptado la axiomática de Huntington, este teorema 8 (que es el A_{10} de Birkhoff-McLane) habrá de demostrarse, arrancando de la equivalencia [1] del número 2.15.

Se establece una relación Ω sobre A

$$a \,\Omega\, b \Leftrightarrow (a \perp b = a) \wedge (a * b = b),$$

que se procede a demostrar que es de orden.

1.º Ω es reflexiva sobre A: $a \,\Omega\, a$, $\forall a \in A$.

En efecto: según la ley de idempotencia (T_3)

$$(a * a = a) \wedge (a \perp a = a),$$

lo cual es equivalente a $a \,\Omega\, a$.

2.º Ω es antisimétrica sobre A: $\forall a \in A$, $\forall b \in A$, $\left.\begin{matrix} a \,\Omega\, b \\ b \,\Omega\, a \end{matrix}\right\} \Leftrightarrow a \equiv b.$

En efecto: $a \,\Omega\, b \Leftrightarrow a \perp b = a$

$b \,\Omega\, a \Leftrightarrow b \perp a = b.$

Según A_4: $a = a \perp b = b \perp a = b$; es decir: $a \equiv b$;

recíprocamente:

$$a = b \Rightarrow a \perp a = a \perp b;$$

por T_3 (idempotencia), $a = a \perp b \Leftrightarrow a \,\Omega\, b$.

De análoga manera,

$$b = a \Rightarrow b \perp b = b \perp a \quad ; \quad b = b \perp a \Leftrightarrow b \,\Omega\, a$$

3.º Ω es transitiva sobre A: $a \in A$, $b \in A$, $c \in A$,

$$\left.\begin{matrix} a \,\Omega\, b \\ b \,\Omega\, c \end{matrix}\right\} \Rightarrow a \,\Omega\, c$$

En efecto:

$$a \,\Omega\, b \Leftrightarrow a \perp b = a \qquad [1]$$
$$b \,\Omega\, c \Leftrightarrow b \perp c = b \qquad [2]$$

Componiendo miembro a miembro [1] y [2], con $\perp$,

$$(a \perp b) \perp (b \perp c) = a \perp b$$
$$= a \perp (b \perp c).$$

Usando la ley de asociatividad (T_4),

$$[(a \perp b) \perp b] \perp c = a \perp (b \perp c).$$

De nuevo, según T_4,

$$[a \perp (b \perp b)] \perp c = a \perp (b \perp c).$$

Aplicando la ley de idempotencia (T_3) y la hipótesis [2],

$$[a \perp b] \perp c = a \perp b.$$

Según la hipótesis [1],

$$a \perp c = a \Rightarrow a \,\Omega\, c.$$

TEOREMA 9

En un álgebra de Boole ordenada, $[A, *, \perp, \Omega]$, existen extremos absolutos ϕ y U.

Este teorema corresponde al axioma A_{11} de Birkhoff-McLane.

Demostración:

D_1) $\forall a \in A$,
$a \perp \phi = \phi$, según T_1
$\phi \perp a = \phi$, según A_4
$\Updownarrow$
$\phi \,\Omega\, a$

D_2) $a \perp U = a$, según A_7
$\Updownarrow$
$a \,\Omega\, U$

TEOREMA 10

Ley de Dedekind: En toda álgebra de Boole se cumple que si

$$a \,\Omega\, b \Rightarrow a * (c \perp b) \equiv (a * c) \perp b$$

Usando la distributividad (A_6),

$$a * (c \perp b) = (a * c) \perp (a * b).$$

Según la equivalencia [1] de 2.15, la hipótesis $a \,\Omega\, b$ implica que $(a * b) = b$; de modo que sustituyendo, resulta la tesis.

Los retículos que cumplen este teorema 10 suelen recibir el nombre de *módulos*. Es claro que todo retículo distributivo es un módulo, y por extensión, toda álgebra de Boole.

2.17. EL ALGEBRA DE BOOLE DEL «TODO O NADA »

Considérese un conjunto $A = \{\alpha, \beta\}$ cuyos dos únicos elementos distintos están estructurados en álgebra de Boole.

Los teoremas 8 y 9, recientemente demostrados, exigen que A admita una relación de orden parcial Ω, con extremos absolutos. Necesariamente, entonces, los dos únicos elementos de A habrán de ser, precisamente, esos extremos absolutos del orden $[A, \Omega]$.

Entendamos, por ejemplo, que $\alpha \equiv \phi$ y que $\beta \equiv U$.

Las tablas que se establecen son los compendios operativos del álgebra de Boole propuesta:

*	ϕ	U
ϕ	ϕ	U
U	U	U

$\perp$	ϕ	U
ϕ	ϕ	ϕ
U	ϕ	U

	$'$
ϕ	U
U	ϕ

Queda patente la razón del nombre que titula el epígrafe de álgebra de Boole del «todo-nada».

Ejemplo 1

Sea un conjunto unitario $A = \{a\}$. Su conjunto potencia o conjunto de sus partes es

$$\mathcal{P}(A) = \{\phi, \{a\}\}$$

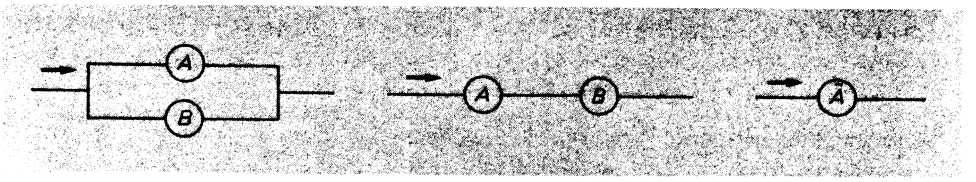
El álgebra de Boole $[\mathcal{P}(A), \cup, \cap, ']$ es un álgebra de Boole del «todo-nada».

Ejemplo 2

Sea el conjunto E el conjunto de los estados conductores de los circuitos, que sólo pueden tener dos estados: conductor y no conductor, y que denotaremos por 1 y 0, respectivamente

$$E = \{0, 1\}$$

Las operaciones binarias, que en conjuntos son la reunión e intersección, aquí son la conexión-paralelo y la conexión-serie; la complementariedad viene representada por el circuito-complementario que, obedeciendo a la tabla de la operación, es el circuito en estado de conducción opuesto al original.



∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	0
1	0	1

	~
0	1
1	0

Ejemplo 3

Sea el conjunto M el conjunto de los valores de verdad de las proposiciones, que como ya se expresó, son dos excluyentes: Verdadero, Falso:

$$M = \{V, F\}$$

Como operaciones binarias en M establecemos la disyunción ($\vee$) y la conjunción ($\wedge$) lógicas, mientras que la complementariedad viene aquí representada por la operación lógica «negación» ($\sim$).

El álgebra de Boole $[M, \vee, \wedge, \sim]$ es también un álgebra de Boole del todo-nada, y sus tablas operativas son idénticas a las del ejemplo segundo: basta signar «Verdad» con 1 y «Falso» con 0, que, por otro lado, es como se hace comúnmente.

2.18. FUNCIONES BOOLEANAS

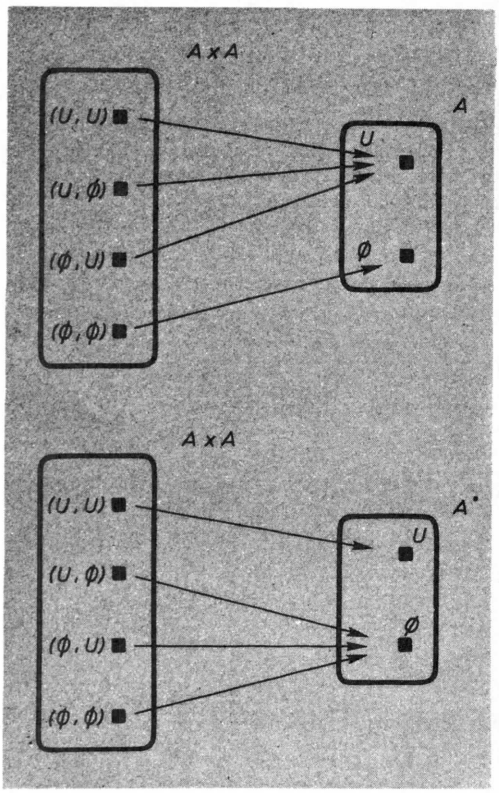
Sea A un conjunto binario estructurado en álgebra de Boole del todo-nada; y sean $x_1, x_2, \ldots, x_i, \ldots, x_n$ letras representantes de variables en A, de modo que pueden tomar «el valor» ϕ o U.

Se denomina función booleana a toda aplicación sobreyectiva* del cartesiano $A \times A \times A \times \cdots$ (n sobre A, de tal manera que cada n-tupla de $A \times A \times A \ldots$ (n tiene por imagen en A uno de sus dos elementos: ϕ o U.

Especifiquemos primero un par de ejemplos de función booleana de dos variables:

$$\boxed{y = x_1 * x_2}$$

* A veces, no sobreyectiva.

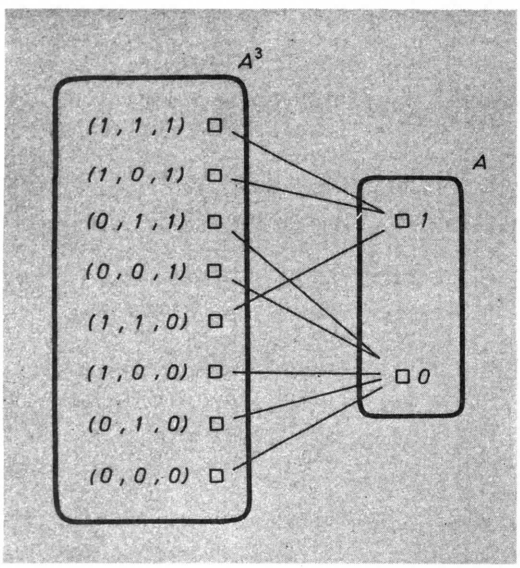


x_1	x_2	$x_1 * x_2$
U	U	U
U	ϕ	U
ϕ	U	U
ϕ	ϕ	ϕ

$$y = x_1 \perp x_2$$

x_1	x_2	$x_1 \perp x_2$
U	U	U
U	ϕ	ϕ
ϕ	U	ϕ
ϕ	ϕ	ϕ

Describamos ahora un tercer ejemplo, esta vez con tres variables. Utilizaremos la notación más extendida para los extremos absolutos $U = 1$ y $\phi = 0$



$$y = x_1 \perp (x_2 * x_3)$$

x_1	x_2	x_3	y
1	1	1	1
1	0	1	1
0	1	1	0
0	0	1	0
1	1	0	1
1	0	0	0
0	1	0	0
0	0	0	0

Finalmente, recordemos que el álgebra de las proposiciones, ya estudiada, se reduce al tratamiento de funciones booleanas lógicas, en las que las variables son los enunciados simples que las constituyen.

NOTA AL LECTOR. Tal vez se haya dado cuenta el lector de lo muy conveniente que resultaría en un aprendizaje cíclico de estos rudimentos del Algebra, el «reciclar» lecturas; se quiere decir que ahora, a la luz del establecimiento abstracto de la estructura del álgebra de Boole, cobran toda su dimensión los tratamientos no formalizados con que se describieron monográficamente los modelos que preceden: el álgebra de conjuntos y el álgebra de las proposiciones. Un estudio consecuente exigiría la relectura de lo anterior, consiguiéndose con ello la plenitud de un aprendizaje inductivo-deductivo-inductivo.

2.19. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

2.190.

Sobre el álgebra de Boole del conjunto de los conjuntos se establece la operación

$$A \$ B = (A \cup B) - (A \cap B)$$

Demuéstrese que la ley establecida es asociativa.

2.191.

En el álgebra de Boole del todo-nada se crea la operación

$$a \,\&\, b = (a \cap b') \cup (a' \cap b)$$

Constrúyase su tabla de resultados.

2.192.

Justifíquese que el conjunto $A = \{1, 2, 6, 7, 21, 42\}$ es un retículo para la relación de divisibilidad x/y. Muéstrense los límites superior e inferior de $A \subset N$.

2.193.

Sea A un referencial y $\mathcal{P}(A)$ el conjunto de sus partes, estructurado en forma de retículo.

Considérense los conjuntos unitarios $\{a\} \in \mathcal{P}(A)$ y sea un $\{b\} \in \mathcal{P}(A)$, distinto de ϕ.

El retículo $\mathcal{P}(A)$ se denomina *atómico* si cumple esta condición:

$$\phi \subset \{b\} \subset \{a\} \Rightarrow \{b\} \equiv \{a\}$$

2.194.

Sea $M = \{\{m_1\}, \{m_2\}, \ldots, \{m_z\}\}$ el conjunto de los conjuntos de múltiplos de $\forall m \in Z$.

Se establecen sobre M dos operaciones:

1.ª *Adición*

$$\{m_i\} + \{m_j\} = \{m_k\},$$

de modo que los elementos de m_k son los formados por la adición de cada elemento de m_i con cada uno de los de m_j;

2.ª *Intersección*

$$\{m_i\} \cap \{m_j\} = \{m_k\},$$

siendo los elementos de m_k los múltiplos del m.c.m. de m_i y m_j.

A) Justifíquese que la terna $[M, +, \cap]$ es un retículo.

B) Demuéstrese que ese retículo no es atómico.

2.195.

Se considera el conjunto P de todos los puntos y rectas del plano, y se definen sobre P dos operaciones:

1.ª *Reunión*: conjunto de todos los puntos determinados por las rectas que unen dos a dos cada uno de los puntos de los elementos reunidos;

2.ª *Intersección*: conjunto de puntos comunes a los elementos interesados.

A) Justifíquese que la terna $[P, \cup, \cap]$ es un retículo.

B) Demuéstrese que no alcanza la estructura de álgebra de Boole.

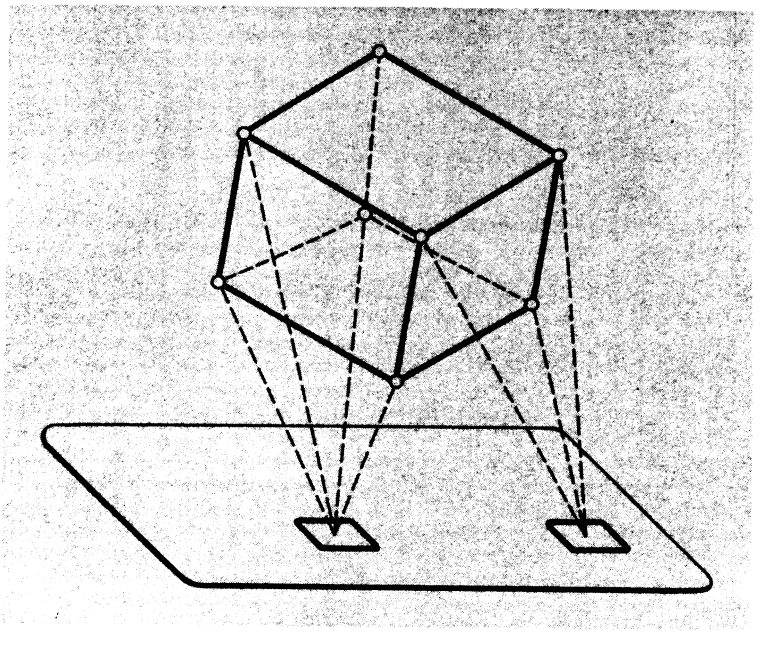
2.196.

1.º Sobre ejes rectangulares constrúyase la gráfica de la función lineal $y = 1/2 \cdot x$.

2.º También realícese la misma representación sobre dos ejes paralelos.

3.º Sobre el triedro ortonormal represéntese la función $z = 3x - y$.

4.º De igual modo, represéntese la función booleana del ejemplo primero del número 2.18.



2.197.

Interprétese la figura «muda» adjunta, nombrando los puntos representativos, dominios y codominios, como una representación de la función booleana del ejercicio tercero del número 2.19.

2.198.

Un piloto está encendido en un panel, si los dos pulsadores que lo accionan no están pisados; se apaga si se pisa uno cualquiera de los dos, pero se mantiene encendido si se pulsan simultáneamente ambos. Llamando a cada uno de los pulsadores x_1 y x_2, establecer:

1.º La tabla de resultados de la función booleana $y = f(x_1, x_2)$;
2.º Comprobar que se corresponde con la de la función

$$y = (x_1 \wedge x_2) \vee (x_1' \wedge x_2')$$

2.199.

Paradoja de Hempel. En la teoría de conjuntos existe la equivalencia $A \subseteq B \equiv B' \subseteq A'$. Muéstrese mediante un diagrama de Venn.

Pero

$$A \subseteq B \Rightarrow x \in A \Leftrightarrow x \in A \cap B;$$

además:

$$B' \subseteq A' \Rightarrow x \in B' \Leftrightarrow x \in B' \cap A'.$$

Ilústrese esta paradoja con algún ejemplo sencillo.

2.2

Correspondencias

2.21. El concepto de correspondencia a partir del de relación

2.22. Nomenclatura y representación

2.23. Correspondencia recíproca o inversa de otra

2.24. Clasificación de correspondencias. Aplicaciones

2.25. Funciones: un cuadro de sinónimos

2.26. Producto de correspondencias

2.261. *Definición*
2.262. *Producto de aplicaciones*

2.2621. Condición de composición
2.2622. Teorema 1
2.2623. Teorema 2
2.2624. Teorema 3
2.2625. Aplicación inversa de otra
2.2626. Restricción de una aplicación

2.27. Conjunto de aplicaciones entre conjuntos finitos. Combinatoria

2.271. *Potencia del conjunto de aplicaciones entre dos conjuntos finitos: variaciones con repetición*
2.272. *Potencia del conjunto de inyecciones entre dos conjuntos finitos: variaciones*
2.273. *Potencia del conjunto de biyecciones entre dos conjuntos finitos: permutaciones*
2.274. *Combinaciones sin repetición*
2.275. *Anexo de cálculo combinatorio*

2.2751. Permutaciones circulares
2.2752. Permutaciones con repetición
2.2753. Combinaciones con repetición

2.28. Primera noticia de dos sugestivos conceptos: categorías y functores

2.29. Aplicabilidad. Automatismos y destrezas

2.2

Correspondencias

2.21. EL CONCEPTO DE CORRESPONDENCIA A PARTIR DE RELACION

Considérese el cartesiano $A \times B$ y, en él, el grafo G de una relación R:

$$G \subset A \times B$$

$$G = \{(a, b)/a\ R\ b\}$$

Se plantea también el retículo de las partes de B, $P(B)$, y se crea un nuevo grafo $\bar{f} \subset A \times P(B)$, cuyos pares ordenados tienen como primeras proyecciones los $a \in A$ y como segundas, los subconjuntos del retículo $P(B)$:

$$\bar{f} = \{(a, \{p(B)\})/a\ R\ b,\ \forall b \in \{p(B)\}\}$$

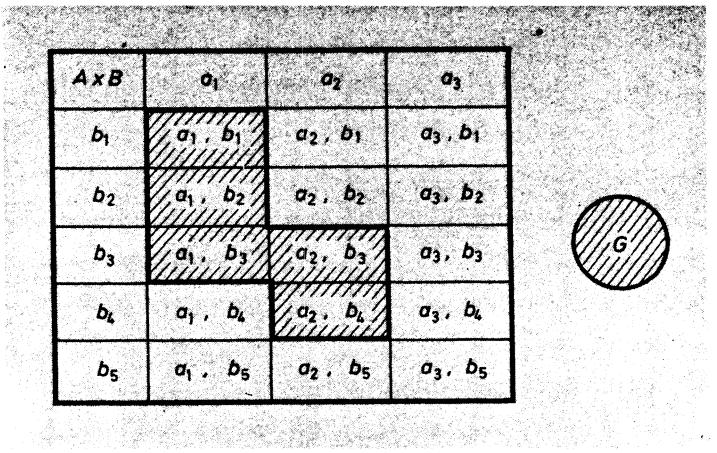
El grafo $\bar{f}$, así establecido, define una correspondencia entre los conjuntos A y B.

Para facilitar la comprensión de la definición abstracta, describimos lo establecido con un sencillo ejemplo finito

$$A = \{a_1\ a_2, a_3\};$$

$$B = \{b_1, b_2, b_3, b_4, b_5\}$$

$$G = \{(a_1, b_1);\ (a_1, b_2);\ (a_1, b_3);\ (a_2, b_3);\ (a_2, b_4)\}$$



Ahora establecemos el retículo $P(B)$, en sus $2^5 = 32$ elementos:

$$P(B) = \{\phi,\ \{b_1\},\ \{b_2\},\ \ldots,\ \{b_1, b_2\},\ \ldots,\ \{b_3, b_4\},\ \ldots,\ \{b_1, b_2, b_3\},\ \ldots,\ \{B\}\}$$

En el grafo de la correspondencia $\bar{f}$ acompañarán

a la primera proyección a_1 el subconjunto $\{b_1, b_2, b_3\} \equiv B_1$
a la primera proyección a_2 el subconjunto $\{b_3, b_4\} \equiv B_2$
a la primera proyección a_3 el subconjunto ϕ,

de modo que el grafo de la correspondencia resulta

$$\bar{f} = \{(a_1, B_1);\ (a_2, B_2);\ (a_3, \phi)\}$$

2.22. NOMENCLATURA Y REPRESENTACION

Es muy conveniente que el lector comprenda que el concepto de correspondencia se puede establecer de muy diversos modos. Nosotros nos decidimos por basarle en el de relación, cuando otros autores construyen a la inversa: crean el concepto de relación a partir del de correspondencia. Se quiere resaltar que el concepto de correspondencia (y el de función, su inmediata y más rica consecuencia) es concepto básico en la Matemática, y que no tiene ninguna servidumbre respecto de otros, al margen de que se introduzca de esa o aquella manera.

En lenguaje usual diremos que la correspondencia f transforma los elementos del conjunto A en elementos del B, y la escritura toma la forma

$$f(A) = B_I,$$

estando $B_I \subset B$, formado por las segundas proyecciones de R.

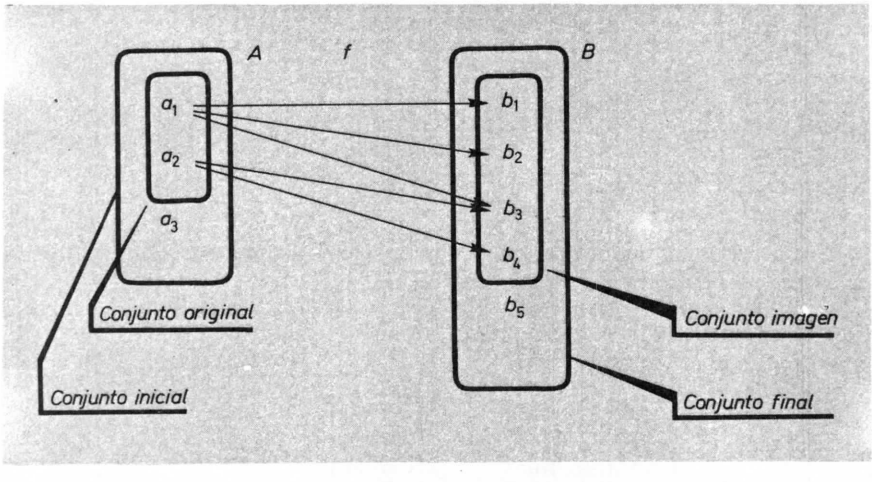
En el ejemplo que venimos estableciendo,

$$f(a_1) = \{b_1, b_2, b_3\}$$
$$f(a_2) = \{b_3, b_4\}$$
$$f(a_3) = \phi$$

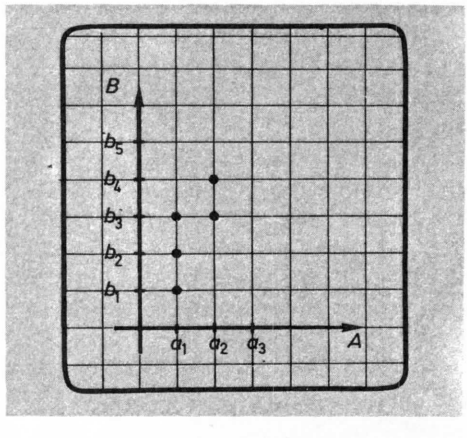
Se denomina *conjunto inicial* de la correspondencia al primer factor A del cartesiano sobre el que está definida, mientras que recibe el nombre de *conjunto original* el $A_1 \subset A$, formado por las primeras proyecciones del grafo G.

A su vez, se llama *conjunto final* el segundo factor del cartesiano $A \times B$. Recibe el nombre de *conjunto imagen* el conjunto-reunión de todas las segundas proyecciones de f, que coincide con el conjunto de las segundas proyecciones de R, B_I.

Sensibilicemos sobre el ejemplo:



Para representar una correspondencia se utiliza el diagrama cartesiano que —supuesto harto conocido a estas alturas de aprendizaje— establecemos a continuación sobre el ejemplo propuesto, sin más explicación.



2.23. CORRESPONDENCIA RECIPROCA O INVERSA DE OTRA

Considérese el cartesiano $B \times A$ y en él, el grafo G^{-1} de la relación R^{-1}, recíproca de la R, establecida anteriormente.

Una idéntica construcción a la realizada antes para f, lleva a crear la correspondencia inversa f^{-1}:

$$G^{-1} \subset B \times A$$
$$G^{-1} = \{(b, a)/a\ R\ b\}$$
$$\bar{f}^{-1} = \{(b, \{p(A)\}/a\ R\ b,\ \forall a \in \{p(A)\}\}$$

El grafo $\bar{f}^{-1}$, así establecido, define la correspondencia inversa de la f, entre los conjuntos B y A.

En el ejemplo que nos viene sirviendo de concreción resultará:

$$f^{-1}(b_1) = \{a_1\}$$
$$f^{-1}(b_2) = \{a_1\}$$
$$f^{-1}(b_3) = \{a_1, a_2\}$$
$$f^{-1}(b_4) = \{a_2\}$$
$$f^{-1}(b_5) = \phi$$

Es claro que en la correspondencia inversa f^{-1}, los conjuntos implicados cambian «su oficio y nombre», según la siguiente tabla:

en f	*en* f^{-1}
Conjunto inicial	Conjunto final
Conjunto original	Conjunto imagen
Conjunto final	Conjunto inicial
Conjunto imagen	Conjunto original

2.24. CLASIFICACION DE CORRESPONDENCIAS. APLICACIONES

La idea de correspondencia toma su mayor entidad en una restricción de su concepto: el de aplicación.

Aplicación es una correspondencia cuyo grafo $\bar{f}$ tiene por primeras proyecciones todos los elementos del conjunto inicial y las segundas proyecciones de sus pares son subconjuntos unitarios del retículo de las partes del conjunto final.

La definición escrita, del todo consecuente con el planteamiento anterior, sin embargo nada tiene de usual a estos niveles. Mejor sería, tal vez, fijar el concepto en los términos más comunes del aprendizaje medio, del que —suponemos— procede el lector.

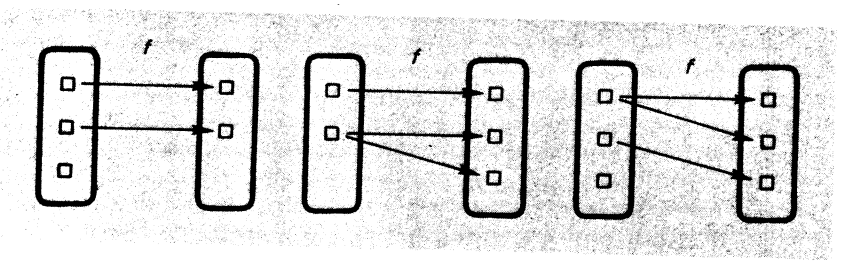
Aplicación es una correspondencia en la que para todo elemento del conjunto inicial existe una y sólo una imagen en el conjunto final.

De un modo u otro, el lenguaje matemático, universal y preciso, establece el concepto de aplicación así:

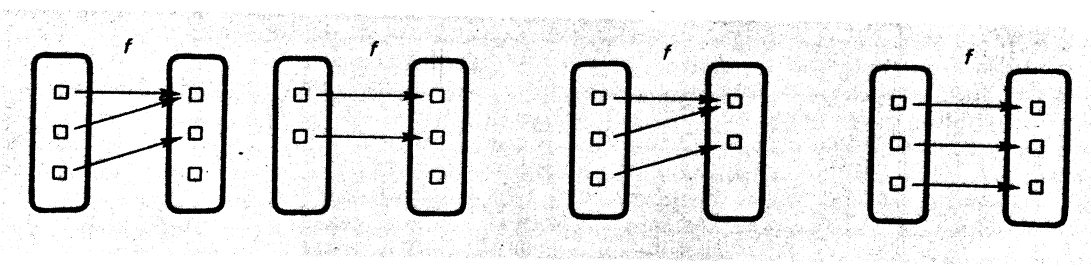
$$\left.\begin{array}{l} f\colon A \to B \text{ es} \\ \text{aplicación} \end{array}\right\} \Leftrightarrow \forall a \in A,\ \exists^* b \in B / f(a) = b$$

Se ha respetado la costumbre de omitir las llaves indicativas del conjunto unitario $\{b\}$, abreviación universal para cuando las segundas proyecciones (imágenes) de las correspondencias son conjuntos unitarios.

No nos parece ingenuo intercalar aquí las típicas figuras de aprendizajes anteriores que aseguren la fijación del concepto



Correspondencias
NO aplicaciones



Aplicaciones

Las aplicaciones pueden ser de varias clases: inyectivas, exhaustivas* y biyectivas.

Establecemos los tres conceptos y debajo proporcionamos las apoyaturas gráficas que se acostumbran en aprendizajes iniciadores.

Aplicaciòn inyectiva es la aplicación en la que cada imagen lo es de un solo antecedente. Es decir:

$$\left.\begin{array}{l} \text{La aplicación} \\ f\colon A \to B \\ \text{es inyectiva} \end{array}\right\} \Leftrightarrow \forall b \in f(A),\ \exists^* a \in A / f(a) = b$$

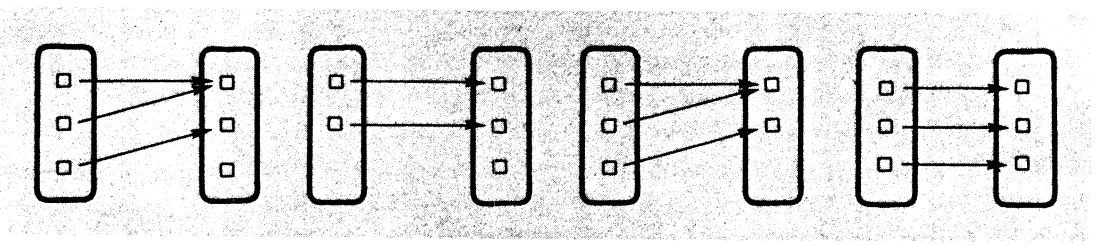
* También llamadas suprayectivas o sobreyectivas.

Aplicación exhaustiva es la aplicación en la que el conjunto imagen coincide con el conjunto final. O sea:

$$\left.\begin{array}{l}\text{La aplicación} \\ f\colon A \to B \\ \text{es exhaustiva}\end{array}\right\} \Leftrightarrow \forall b \in B,\ \exists a \in A / f(a) = b$$

Aplicaciòn biyectiva es la aplicación simultáneamente inyectiva y exhaustiva. Simbólicamente:

$$\left.\begin{array}{l}\text{La aplicación} \\ f\colon A \to B \\ \text{es biyección}\end{array}\right\} \Leftrightarrow \forall b \in B,\ \exists^* a \in A / f(a) = b$$



A. | no inyectiva, no exhaustiva | inyectiva, no exhaustiva | no inyectiva, exhaustiva | biyectiva

Todavía estableceremos dos adjetivos más para las aplicaciones:

Aplicación idéntica es aquella en la que el conjunto inicial y final coinciden y en la que cada elemento es imagen de sí mismo; es decir:

$$\left.\begin{array}{l}\text{La aplicación} \\ f\colon A \to B \\ \text{es A. idéntica}\end{array}\right\} \Leftrightarrow (B \equiv A) \wedge (\forall a \in A,\ f(a) = a)$$

Aplicación constante. Recibe este nombre toda aplicación cuyo conjunto-imagen es unitario; o bien,

$$\left.\begin{array}{l}\text{La aplicación} \\ f\colon A \to B \\ \text{es A. constante}\end{array}\right\} \Leftrightarrow \text{card } f(A) = 1$$

2.25. FUNCIONES: UN CUADRO DE SINONIMOS

Función es una correspondencia entre conjuntos numéricos en la que el conjunto inicial coincide con el original; es decir, todos los elementos de A han de tener, al menos, una imagen*

$$\left.\begin{array}{l} f: A \to f(A) \\ \text{es función} \end{array}\right\} \Leftrightarrow \forall x \in A,\ \exists y \in f(A)/y = f(x)^{**}$$

Obsérvese que, siguiendo el uso del análisis, el conjunto final no se considera y se define sobre el conjunto de imágenes $f(A)$. Si se admite esto, toda función es de tipo exhaustivo. De cualquier modo, es una simple cuestión de convenio.

El capítulo de funciones posee lenguaje propio, consagrado por el uso del análisis. Entendemos que son suficientes los dos cuadros comparativos que se facilitan para zanjar la cuestión sin más prolijas descripciones; pero advierta el lector que ha de ser capaz de establecer cualquier concepto en «lenguaje de funciones», sin más que trasladar el correspondiente establecido en correspondencias. Además, si desea o necesita más extensa descripción, le remitimos al capítulo correspondiente de este libro, en el que, desde un punto de vista analítico, se trata cumplidamente.

Sólo nos queda decir a este respecto que los autores que excluyen las funciones multiformes del concepto de función las consideran como «colecciones de funciones uniformes», representadas en cada una de sus «ramas» (véase el punto 3.54 de Análisis básico.

2.26. PRODUCTO DE CORRESPONDENCIAS

2.261. Definición

Sea R una relación entre A y B, y f la correspondencia que genera. Considérese otra relación S entre los conjuntos B y C, siendo g su correspondencia asociada.

Se establece el producto de relaciones $R \times S = T$, entre los elementos de A y de C. La correspondencia asociada a T la definimos como el producto de correspondencias f y g; la denotamos h y escribimos:

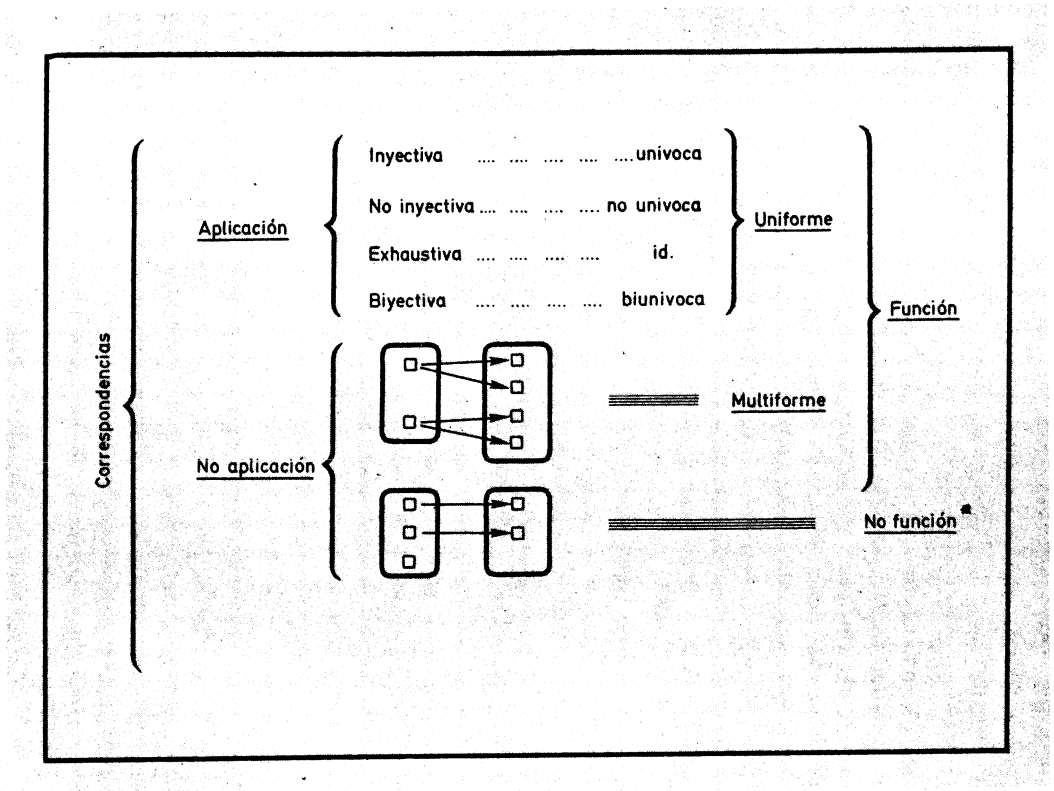
$$h = g \times f$$

Adviértase el orden de factores. El hecho de «escribirlos al revés» no es caprichoso, sino que responde a la manera natural de producirse la composición. Véase

---

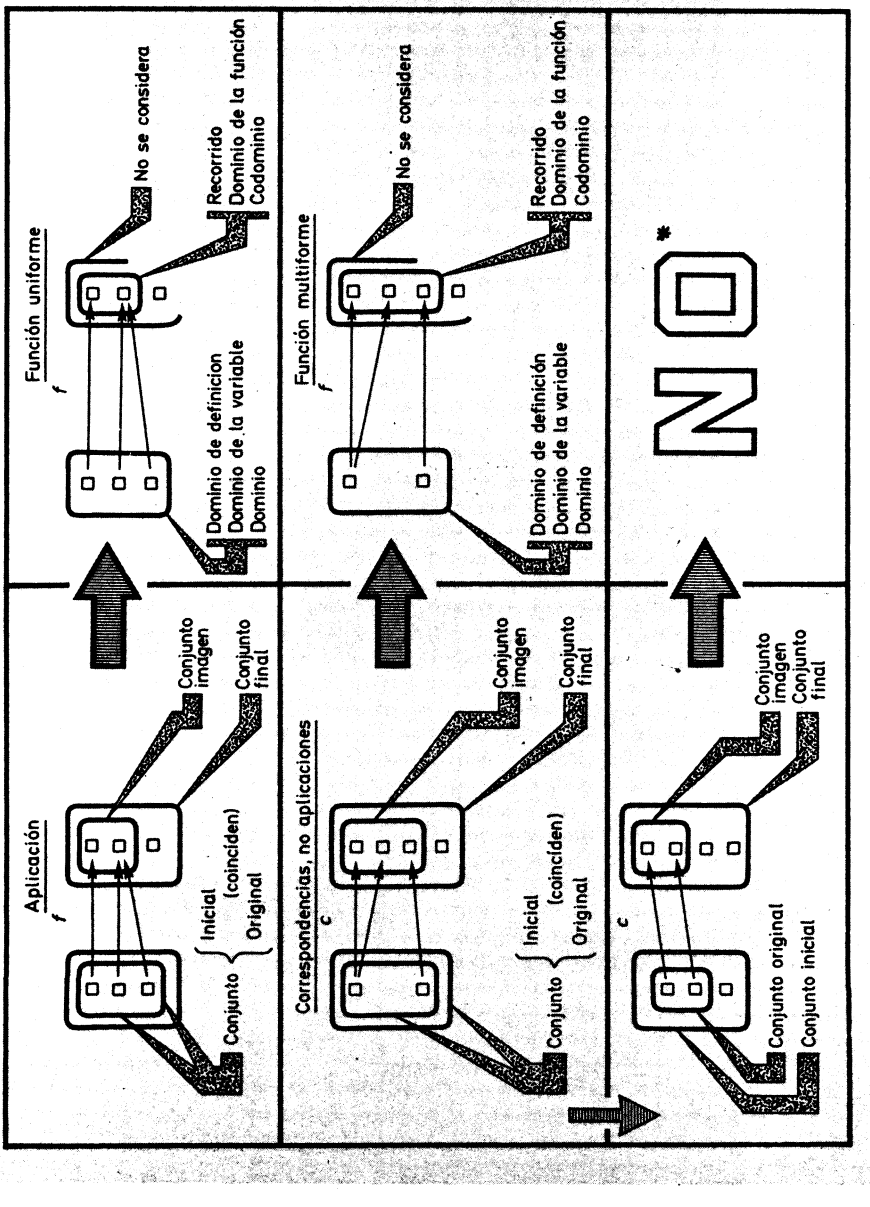
* Si encuentra alguna diferencia con otras definiciones, entienda que nosotros lo hacemos así con el fin —exclusivamente didáctico— de poder hablar cuando llegue el momento de «funciones multiformes», sin restricción alguna, como tales funciones. Estamos convencidos que los cuadros *adjuntos* le serán absolutamente esclarecedores de estas —insistimos— simples cuestiones de convenio de nomenclatura.

** Por razón didáctica queda escrita la última igualdad de la definición que, en purismo matemático, es superflua.



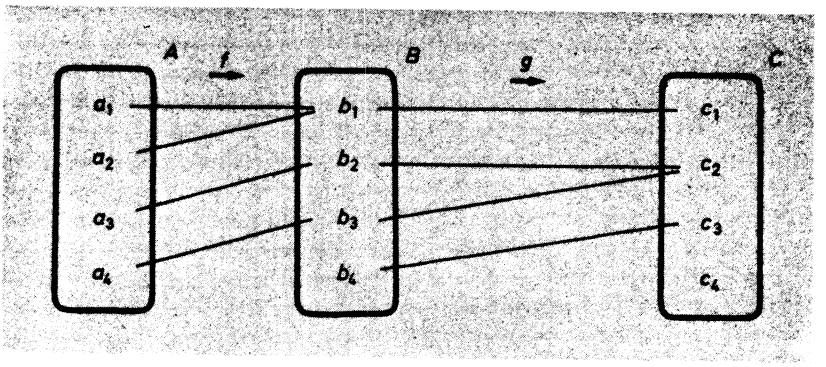
CORRESPONDENCIAS Y APLICACIONES-FUNCIONES

* Para otros autores —los más— *función* es sinónimo de aplicación, que puede o no estar definida en todo el conjunto inicial. Sin embargo, entendemos que lo que se sacrifica del modo tradicional de clasificación se gana, con mucho, en la primera didáctica de estas cuestiones. Téngase en cuenta, por otra parte, que cuando se tiene una función definida al modo usual, cuyo conjunto inicial no coincida con el original, basta restringir su dominio para que caiga, del todo, dentro de nuestro establecimiento.



* Véase nota anterior.

sobre el ejemplo que se desarrolla que primero se aplica f y después, a la imagen producida, g.



$$\begin{array}{llll} f(a_1) = b_1 & f(a_2) = b_1 & f(a_3) = b_2 & f(a_4) = b_3 \quad [1] \\ g(b_1) = c_1 & g(b_1) = c_1 & g(b_2) = c_2 & g(b_3) = c_2 \quad [2] \end{array}$$

Sustituyendo [1] en [2]:

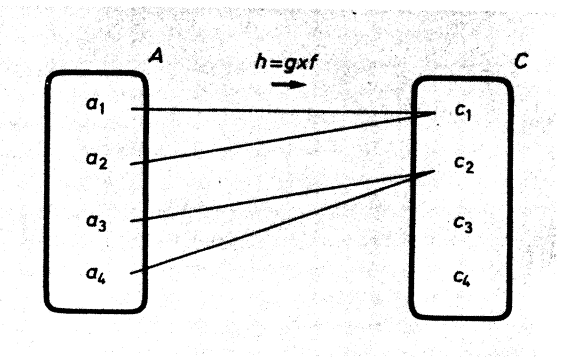
$$g[f(a_1)] = c_1 \qquad g[f(a_2)] = c_1 \qquad g[f(a_3)] = c_2 \qquad g[f(a_4)] = c_2$$

Lo que denotamos:

$$g \times f(a_1) = c_1;\ g \times f(a_2) = c_1;\ g \times f(a_3) = c_2;\ g \times f(a_4) = c_2$$

Siendo $h = g \times f$,

$$h(a_1) = c_1;\ h(a_2) = c_1;\ h(a_3) = c_2;\ h(a_4) = c_2$$



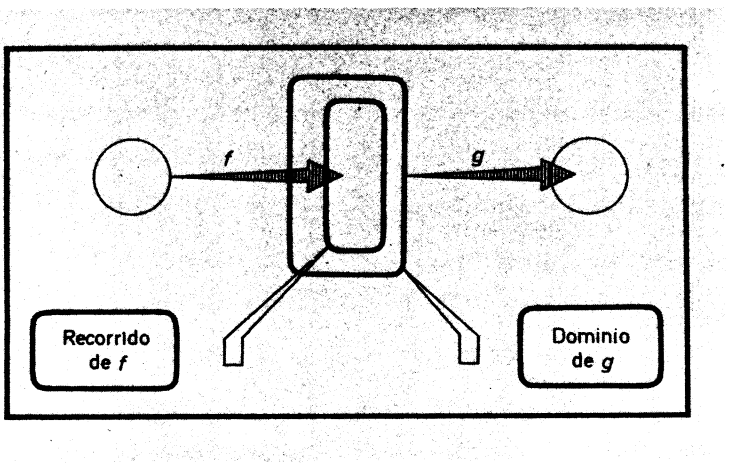
Finalmente, consecuentes con el desarrollo que venimos estableciendo, se escribe el grafo $\bar{h}$ de la correspondencia producto $h = g \times f$, que la define:

$$\bar{h} = \{(a,\ \{p(C)\})/a\ T\ c,\ \forall c \in \{p(C)\}\}$$

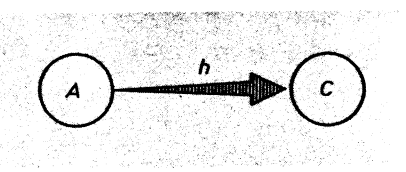
2.262. Producto de aplicaciones

2.2621. *Condición de composición*

No todas las aplicaciones pueden componerse. Para poder llevar a cabo su producto es necesario que el conjunto-imagen de la primera sea un subconjunto del conjunto-original de la segunda; o utilizando vocabulario de funciones, que el recorrido de la primera esté incluido en el dominio de la segunda, tal como pretende expresar el siguiente esquema:



De este modo, es posible que la función g actúe sobre cualquier $f(x)$ que le sirva f; y $g \times f(x)$ seguirá siendo una aplicación de A en C



Ejercicio. Justifíquese que —en efecto— el producto de dos aplicaciones que cumplen esta condición es otra aplicación.

2.2622. Teorema 1

El producto de dos aplicaciones inyectivas es una inyección.
En efecto: sean las inyecciones

$$f\colon A \to B \Leftrightarrow \forall b \in f(A),\ \exists^* a \in A/f(a) = b \qquad [1]$$
$$g\colon B \to C \Leftrightarrow \forall c \in g(B),\ \exists^* b \in B/g(b) = c \qquad [2]$$

De [1] y [2], teniendo en cuenta la condición $f(A) \subset B$, se puede escribir

$$\forall c \in g[f(A)],\ \exists^* a \in A/g[f(a)] = c;$$

o lo que es igual:

$$\forall c \in g \times f(A),\ \exists^* a \in A/g \times f(a) = c;$$

y si denotamos $g \times f = h$,

$$\forall c \in h(A),\ \exists^* a \in A/h(a) = c,$$

que establece como inyección la aplicación $h\colon A \to C$.

Corolario: El producto de dos biyecciones es una biyección. Basta incorporar a los razonamientos anteriores las identidades $f(A) \equiv B$ y $g(B) \equiv C$.

2.2623. TEOREMA 2

El producto de aplicaciones, en general, no es conmutativo.

Para demostrar una proposición negativa universal, basta establecer un antiejemplo, como el que sigue:

Sean las funciones reales de variable real

$$R \to R\colon f(x) = x + 2$$
$$R \to R\colon g(x) = x^2$$

Determinemos la imagen del real 3 en ambos productos:

$$g \times f(3) = g[f(3)] = g(3 + 2) = g(5) = 25$$
$$f \times g(3) = f[g(3)] = f(3^2) = f(g) = 11$$
$$g \times f(3) \neq f \times g(3)$$

2.2624. TEOREMA 3

El producto de aplicaciones es asociativo.
Hipótesis: $f\colon A \to B$
$g\colon B \to C$
$h\colon C \to D$ son tres aplicaciones, componibles dos a dos. Además:
$f(a) = b;\ g(b) = c;\ h(c) = d.$

Tesis: $\forall a \in A,\ h \cdot (g \cdot f)[a] = (h \cdot g) \cdot f[a]$.

Demostración:

$$h \cdot (g \cdot f)[a] = h \cdot [(g \cdot f)(a)] = h[g(f(a))] = h[g(b)] = h(c) = d$$
$$(h \cdot g) \cdot f[a] = (h \cdot g)[f(a)] = h \cdot g(b) = h[g(b) = h(c) = d$$

Ejercicio. Realícese el esquema correspondiente a la demostración.

2.2625. *Aplicación inversa de otra*

Establecimiento: Dada la aplicación biyectiva $f: A \to B$, se dice que $f^{-1}: B \to A$ es su inversa si el producto de ambas es la aplicación idéntica I.

$$f^{-1} \times f \equiv I$$

De modo que: $f^{-1}[f(x)] = f[f^{-1}(x)] = I(x) \equiv x, \ \forall x \in A$

TEOREMA: La condición necesaria y suficiente para que una aplicación tenga inversa es que sea biyectiva*.

Condición necesaria

H. f^{-1} es aplicación; es decir:

$$\forall b \in B, \ \exists^* a \in A / f^{-1}(b) = a$$

T. f es biyectiva; o sea:

$$\forall b \in B, \ \exists^* a \in A / f(a) = b$$

Condición suficiente

H. f es biyectiva; o sea:

$$\forall b \in B, \ \exists^* a \in A / f(a) = b$$

T. f^{-1} es aplicación; es decir:

$$\forall b \in B, \ \exists^* a \in A / f^{-1}(b) = a$$

Demostración: Incorporando a las hipótesis esta doble implicación

$$f^{-1}(b) = a \Leftrightarrow f(a) = b,$$

resulta:

$$\forall b \in B, \ \exists^* a \in A / f(a) = b$$

que no es más que el establecimiento de f como biyección.

$$\forall b \in B, \ \exists^* a \in A / f^{-1}(b) = a$$

que equivale a afirmar que f^{-1} es una aplicación.

2.2626. *Restricción de una aplicación***

Con frecuencia nos encontramos con dos funciones f y g que, por no cumplir la condición de composición, no es posible su producto y, sin embargo, interesaría mucho conseguirlo, al menos, en la «parte que fuera factible».

Si $f(A) \not\subset B$, ¿es posible realizar el producto, considerando solamente la intersección $f(A) \cap B$? Lo es, realizando una restricción de f.

Sea la aplicación $f: A \to B$ y considérese un $B_1 \subset B$. Se denomina restricción de f a B_1 a la función

$$f': A_1 \to B_1 / A_1 = \{x / (x \in A) \wedge (f(x) \in B_1)\}$$

* En análisis es frecuente encontrar este teorema, exigiendo que la función ha de ser simplemente inyectiva. Es cuestión de establecimientos previos. Recuerde el lector lo que se indica en 2.25, respecto de la costumbre de considerar todas las funciones exhaustivas, al definirlas sobre su conjunto-imagen.

** Indistintamente utilizaremos los términos de aplicación y función, naturalmente este último en su acepción de uniforme.

Este nuevo concepto permite abordar la cuestión que lo suscitó: el producto de funciones no componibles. (Véanse diagramas.)

Se plantean las funciones

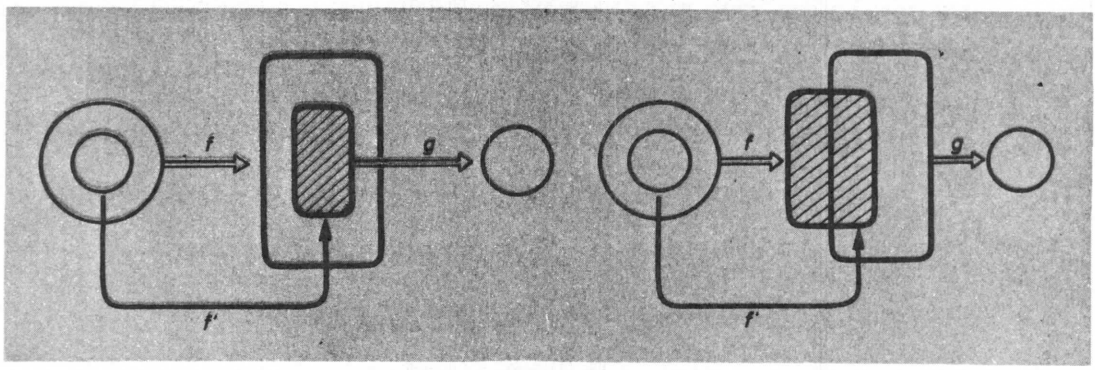
$$f\colon A \to B$$

y

$$g\colon C \to D,$$

siendo

$$(B \not\subset C) \wedge (B \cap C \neq \phi)$$



Se procede a realizar sobre f la restricción siguiente:

$$f'\colon A_1 \to B_1 = B \cap C$$

De este modo, las funciones f' y g son componibles, pudiéndose establecer su producto:

$$g \times f'\colon A_1 \to D$$

Ejemplo

Sean las funciones

$$f\colon N \to Z \quad \text{con} \quad f(x) = 8 - x$$
$$g\colon Z^+ \to R \quad \text{con} \quad g(x) = +\sqrt{x}$$

Sucede que $g \times f(x)$ no existe, ya que g no puede actuar sobre los enteros negativos que le sirve f. Procede hacer una restricción de f a Z^+, de modo que $f(N_1) \subset Z^+$. Es claro que ese subconjunto de los naturales es

$$N_1 = \{1, 2, 3, 4, 5, 6, 7\}$$

Las funciones

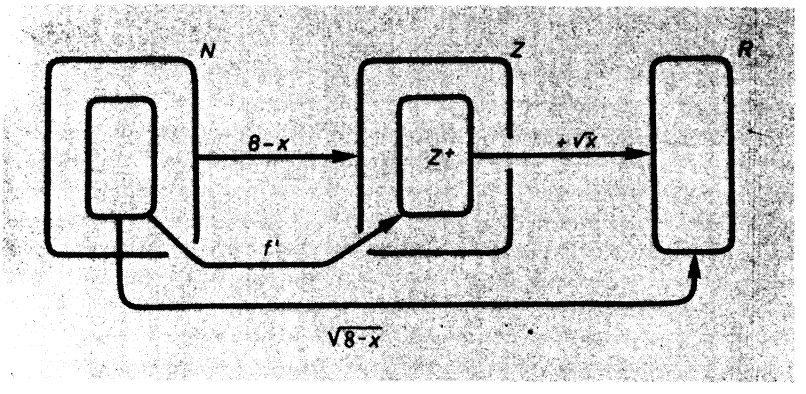
$$f'\colon N_1 \to Z^+$$

y

$$g\colon Z^+ \to R$$

ya tienen producto, que es la función

$$h\colon N_1 \to R \quad \text{con} \quad h(x) = +\sqrt{8-x}$$



2.27. CONJUNTO DE APLICACIONES ENTRE CONJUNTOS FINITOS. COMBINATORIA

2.271. Potencia del conjunto de aplicaciones entre dos conjuntos finitos: variaciones con repetición

Sean A y B dos conjuntos finitos cuyos cardinales son $\text{card}(A) = m$ y $\text{card}(B) = n$; y sea $\mathfrak{F}$ el conjunto de todas las aplicaciones que se pueden establecer sobre ellos.

$$\mathfrak{F} = \{f/f\colon A \to B\}$$

¿Cuál será la potencia o cardinal de $\mathfrak{F}$?

Fijada una imagen para cada $a \in A$, los restantes elementos de A pueden tomar n imágenes distintas; en consecuencia, como son m los elementos de A, se consiguen

$$n \cdot n \cdot n \cdot , \ldots , (m \text{ veces} = n^m \text{ aplicaciones distintas,}$$

$$\text{card}(\mathfrak{F}) = n^m$$

En Combinatoria se establece el concepto de «Variaciones con repetición de n elementos que se pueden repetir hasta m veces» como todas las sucesiones* distintas que se pueden formar, de m términos, usando los n elementos dados.

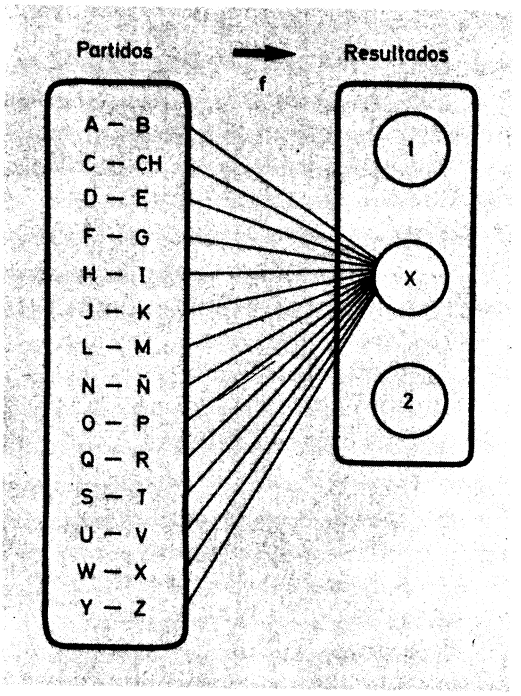
* Basta aquí entender por sucesión un conjunto tabulado en un determinado orden. Además, como $n < m$, necesariamente habrán de repetirse alguno o algunos de los n elementos.

El número de estas sucesiones coincide con el número de aplicaciones, anteriormente fijado, pues cada una de aquéllas viene establecida por el conjunto de las segundas proyecciones de los grafos de éstas. Así, pues,

$$VR_{n,m} = n^m$$

Ejemplo

¿Cuántas quinielas simples han de rellenarse para tener certeza de acierto en los 14 resultados de los partidos?



De todas las aplicaciones entre los dos conjuntos dibujamos una, por cierto, no muy probable: que se consigan catorce empates.

Todas las aplicaciones posibles de los catorce partidos sobre los tres resultados, producirían la certeza de acierto.

Son las variaciones con repetición de tres resultados, que se pueden repetir hasta catorce veces. O sea, el siguiente número de quinielas «muy considerable»:

$$VR_{3,14} = 3^{14} = 4_{1}782.969$$

2.272. Potencia del conjunto de inyecciones entre dos conjuntos finitos: variaciones

Sean A y B dos conjuntos finitos cuyos cardinales son $\text{card}(A) = m$ y $\text{card}(B) = n$; y sea Y el conjunto de todas las aplicaciones inyectivas de A en B

$$Y = \{f/f\colon A \to B\}$$

¿Cuál será la potencia o cardinal de Y?

Fijada una imagen para un $a_1 \in A$, otro $a_2 \in A$, puede tomar $n - 1$ imágenes distintas; determinadas las dos anteriores, un tercer elemento de A puede tomar como imagen a uno de los $n - 2$ elementos que quedan en el conjunto-imagen; y así sucesivamente. De modo que el conjunto de inyecciones posibles viene dado por la fórmula

$$\text{card}(Y) = n \cdot (n-1) \cdot (n-2), \ldots, (n - [m-1])$$

Efectivamente, el último factor del producto es el expresado, pues siendo m el número de antecedentes, al $a_m \in A$, en cada una de las inyecciones, le quedarán para «escoger imagen» en el conjunto de ellas, tantas como la diferencia entre ambos cardinales, exceptuándose él mismo. Con ello, es obvio que el número de factores coincide con m.

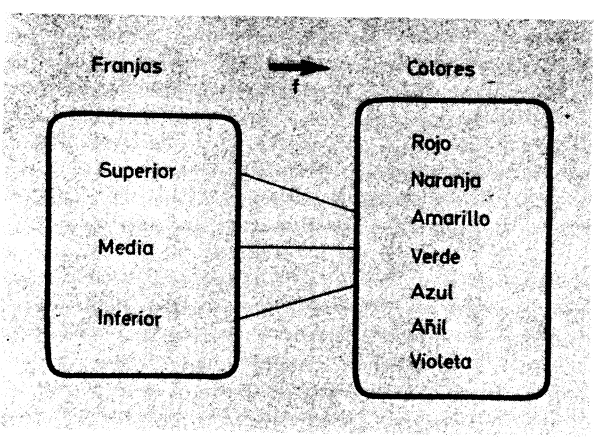
En Combinatoria se establece el concepto de «Variaciones sin repetición de n elementos, que se toman de m en m» como el conjunto de sucesiones distintas de m términos que se pueden formar, usando n elementos dados.

El número de estas sucesiones coincide con el número de inyecciones, anteriormente establecido, pues cada una de aquéllas viene fijada por el conjunto de las segundas proyecciones de los grafos de éstas. Así, pues:

$$V_{n,m} = \underbrace{n \cdot (n-1) \cdot (n-2) \ \ldots \ (n-m+1)}_{m \text{ factores}}$$

Ejemplo

¿Cuántas banderas tricolores de franjas horizontales distintas pueden formarse con los siete colores del espectro visible?



Todas las inyecciones posibles de franjas en colores cubren todos los casos posibles.

Son las variaciones dé siete colores, que se toman de tres en tres.

$$V_{7,3} = 7 \cdot (7 - 1) \cdot (7 - 2) = 210 \text{ banderas}$$

2.273. Potencia del conjunto de biyecciones entre dos conjuntos finitos: permutaciones

El concepto de biyección exige que, establecido entre conjuntos finitos, éstos sean equipotentes (es decir, que tengan igual número de elementos); pero toda biyección es una aplicación inyectiva, de modo que el cálculo realizado en 2.272 es válido para el caso que nos ocupa.

Siendo los conjuntos y símbolos los allí utilizados, y establecido el conjunto de todas las biyecciones de este modo,

$$\mathfrak{B} = \{f/f\colon A \to B\},$$

la potencia del conjunto es

$$\text{card}(\mathfrak{B}) = n \cdot (n - 1) \cdot (n - 2) \ \ldots \ (n - m + 1);$$

pero aquí, como queda dicho anteriormente, $n = m$. Luego:

$$\text{card}(\mathfrak{B}) = n \cdot (n - 1) \cdot (n - 2) \ldots 1$$

$$\text{card}(\mathfrak{B}) = n!$$

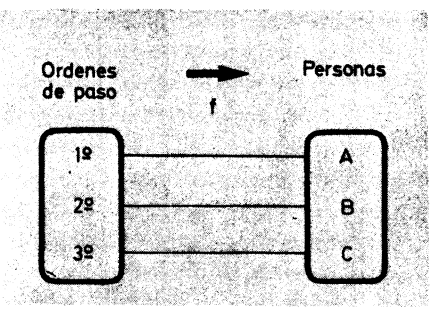
En Combinatoria se establece el concepto de «Permutaciones de n elementos» como el conjunto de sucesiones distintas de n términos que se pueden formar, usando n elementos dados, de modo que la única diferencia posible entre una y otra estriba exclusivamente en el orden.

Es obvio —y su justificación se la dejamos al lector— que el número de permutaciones de n elementos coincide con el de biyecciones posibles entre dos conjuntos de equipotencia n. Así, pues, escribimos:

$$P_n = n!$$

Ejemplo

¿De cuántas formas distintas pueden pasar una puerta abierta tres personas? Todas las biyecciones posibles coinciden con todas las posibilidades de paso.



2.274. Combinaciones sin repetición

Sea el conjunto finito A, formado por n elementos. Considérese el conjunto de sus partes $\mathcal{P}(A)$, que tendrá 2^n elementos.

Se establece un $C_m \subset \mathcal{P}(A)$ formado por todos los subconjuntos de A, de potencia m.

Cada uno de los conjuntos-elemento de C_m se denomina combinación m-aria de n elementos.

Así definido el concepto, es claro que para que dos combinaciones m-arias se consideren distintas, es necesario que, al menos, se diferencien en uno de sus m elementos.

Se puede abordar la determinación del número de ellas, partiendo del número de variaciones m-arias de n elementos, establecido como la potencia del conjunto de inyecciones posibles entre dos conjuntos (2.272).

Del número allí calculado, habrán de deducirse aquellas inyecciones, cuyos conjuntos de segundas proyecciones de sus grafos, sólo se diferencian en el orden de sus elementos. Ello se consigue dividiendo el número de inyecciones por el de biyecciones posibles $f(A) \xrightarrow{f^{-1}} A$, que —como se sabe— es $P_m = m!$ Resulta así

$$C_{n,m} = \frac{V_{n,m}}{P_m} = \frac{n(n-1) \ \ldots \ (n-m+1)}{m!}.$$

Multiplicando arriba y abajo por $(n-m)!$,

$$C_{n,m} = \frac{n!}{m! \cdot (n-m)!}$$

expresión cuyo simbolismo usual es el número combinatorio

$$C_{n,m} = \binom{n}{m}$$

Ejemplo

¿Cuántos colores distintos, compuestos de tres simples, pueden formarse con los siete del espectro visible? (No se tenga en cuenta la complementariedad de colores.)

Supuesto que no importa el orden de mezcla, la pregunta se refiere al número de combinaciones ternarias de siete elementos, de modo que:

$$C_{7,3} = \binom{7}{3} = \frac{7!}{3! \cdot 4!} = 35 \text{ colores compuestos.}$$

2.275. Anexo de cálculo combinatorio

Finalmente, dejamos aquí registradas otras tres cuestiones que —pensamos— serán muy útiles para el estudiante, pues de este modo, tiene localizado de manera

conjunta, en el mismo sitio, un breve y completo recordatorio de cálculo combinatorio.

2.2751. *Permutaciones circulares*

En un orden circular, al ser cerrado, no existen primero y último términos. Dados n elementos, en cada uno de sus posibles órdenes circulares, habrá de dejarse uno fijo, como referencia. De este modo, el número de permutaciones circulares de n elementos es el mismo que el de permutaciones lineales de $n - 1$ elementos. Se escribe, pues:

$$PC_n = (n - 1)!$$

Ejemplo

¿De cuántos modos posibles pueden sentarse a la mesa circular de consejos, los 16 miembros de un gabinete ministerial?

$$PC_{16} = 15! = 1_2307.674_1368.000$$

2.2752. *Permutaciones con repetición*

Si se dispone de n elementos, entre los cuales, uno se repite α veces, otro β veces, etc., y se desean contabilizar todos los posibles órdenes lineales de esos n elementos, en principio, habrá de pensarse en el número de permutaciones de n elementos, $n!$ Pero es claro que en esos órdenes, las permutaciones que se refieren a cambiar entre sí los α elementos iguales, los β iguales, etc., por ser inoperantes, darían los mismos órdenes, de modo que habrá que dividir por el número de «permutaciones internas» de los α, β, etc., elementos iguales.

$$PR_{n,\,(\alpha,\,\beta,\,\ldots)} = \frac{n!}{\alpha! \cdot \beta! \cdot \ldots}$$

Ejemplo

¿Cuántos números distintos de seis cifras se pueden formar con los guarismos 2, 4, 4, 7, 7, 7?

$$PR_{6,\,(2,3)} = \frac{6!}{2! \cdot 3!} = 60 \text{ números}$$

2.2753. *Combinaciones con repetición*

Se demuestra que el conjunto de combinaciones con repetición de n elementos, tomados de m en m, es biyeccionable con el conjunto de combinaciones sin repetición de $n + m - 1$ elementos, tomados de m en m.

Si esto es así, ambos conjuntos son equipotentes, y se verifica:

$$CR_{n,m} = C_{(n+m-1),m} = \binom{n + m - 1}{m}$$

Ejemplo

Calcular el número de números compuestos que se pueden formar, tomando cuatro de los seis primos 2, 3, 5, 7, 11, 13.

Uno de los números pedidos es $2 \times 2 \times 2 \times 2$; otro sería $2 \times 2 \times 3 \times 7$; pero el $2 \times 3 \times 2 \times 7$ no ha de contabilizarse, si se hizo con el anterior. Es claro, pues, que se trata de las combinaciones con repetición de 6 elementos, tomados de 4 en 4.

Su número es:

$$CR_{6,4} = C_{9,4} = \binom{9}{4} = \frac{9!}{4! \cdot 5!} = 504 \text{ números}$$

2.28. PRIMERA NOTICIA DE DOS SUGESTIVOS CONCEPTOS: CATEGORIAS Y FUNCTORES

Intentemos hacer una elevada abstracción, abandonemos de raíz todo soporte intuitivo, e intentemos crear el siguiente universo de discurso, con los siguientes entes matemáticos.

Sea un conjunto O, cuyos elementos son entes matemáticos, que llamaremos *objetos*, cuya única descripción de su naturaleza consiste en decir que son capaces de soportar la acción sobre ellos de otros entes matemáticos.

Considérese también un conjunto M, cuyos elementos toman el nombre de *morfismos* y son entes matemáticos, capaces de acción sobre los «inertes» objetos de O.

Establezcamos la unión de O y M:

$$C = \{\text{Objetos, Morfismos}\}$$

Ahora, obliguemos a C a tener las siguientes propiedades:

P_1) Existe el producto de morfismos; quiere decirse que si A, B y C son tres objetos y f y g dos morfismos que actúan sobre A-B y sobre B-C, respectivamente, resulta que existe un morfismo, capaz de actuar sobre A-C, de igual modo que lo hacen sucesivamente f y g.

P_2) El producto de morfismos es asociativo.

P_3) El hecho de existir un morfismo, implica la existencia de los objetos sobre los que actúa.

P_4) Existen morfismos cuya acción sobre los objetos no los varía: son los morfismos identidad, por la izquierda y por la derecha:

$$\exists I_- \in M,\ \exists I_+ \in M / (I_- \times f = f) \wedge (f \times I_+ = f),\ \forall f \in M$$

Pues bien: recibe el nombre de *categoría* el conjunto C, dotado de las cuatro propiedades establecidas.

La primera categoría concreta que responde a este sugestivo planteamiento la constituyen los objetos llamados *conjuntos* y los morfismos denominados *aplicaciones* sobre ellos. En efecto: el conjunto

$$C = \{\text{conjuntos, aplicaciones}\}$$

por cumplir las cuatro propiedades establecidas, es una *categoría*.

Demos un paso más en la teoría abstracta de las categorías.

Sean dos categorías $C_1 = \{A, M\}$ y $C_2 = \{B, N\}$ y φ una aplicación entre ellas, de modo que:

$$\forall a \in A,\ \varphi(a) = b \in B$$
$$\forall f \in M,\ \varphi(f) = f' \in N$$

Considérense ahora dos objetos a_1 y a_2 de C_1 y $f \in M$, un morfismo de a_1 en a_2.

La aplicación φ, actuando sobre esos elementos descritos, produce sus imágenes en la segunda categoría C_2:

$$\varphi(a_1) = b_1 \in B$$
$$\varphi(a_2) = b_2 \in B$$
$$\varphi(f) = f' \in N;$$

si sucede que:

1.º f' es morfismo de b_1 en b_2;
2.º $\varphi(I_a) = I_b = I_{\varphi(a)}$;
3.º siendo $f_1 \in M$ y $f_2 \in M$,

$$\varphi(f_1) \times \varphi(f_2) = \varphi(f_1 \times f_2),$$

entonces se dice que la aplicación φ es un *functor* de la primera en la segunda categorías.

Tal vez, con lo expuesto, se haya llegado a sospechar la fecundidad de esta teoría de categorías y functores, espléndido camino abierto del álgebra abstracta.

2.29. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

2.290.

Dados los conjuntos $A \equiv B \equiv \{1, 2, 3, 4, 5\}$, establézcase la correspondencia asociada a la relación de orden estricto $<$. Establézcase el grafo de la correspondencia recíproca.

2.291.

Justifíquese que la correspondencia f: $Z \to Z$, con $f(x) = 2 \cdot x$ es una función uniforme unívoca.

2.292.

Sean las funciones

$$f\colon N \to N, \text{ con } f(x) = 3x$$
$$g\colon N \to N, \text{ con } g(x) = 2^x$$

Determínense los productos $g \times f$ y $f \times g$.

2.293.

Sobre cuatro diagramas cartesianos dibuje las representaciones de las funciones siguientes:

$$N \to N\colon f(x) = x^2 + 1$$
$$Z \to Z\colon g(x) = x^2 + 1$$
$$Q \to Q\colon h(x) = x^2 + 1$$
$$R \to R\colon j(x) = x^2 + 1$$

Describa las diferencias que encuentre en esas gráficas.

2.294.

Determine qué clases de funciones son las establecidas en el número anterior. Fije previamente, sus dominios y recorridos.

2.295.

Establézcanse las correspondencias numéricas recíprocas de las cuatro del número 2.293. Represéntense (en otro color) sobre los mismos diagramas. Decídase, razonadamente, cuáles de las correspondencias recíprocas son funciones inversas de las primitivas correspondientes. Sobre los mismos diagramas, represente la función idéntica en cada uno de los dominios y recorridos establecidos y, luego, explicite las simetrías que sorprenda.

2.296.

Entendiendo como lícita la inclusión de inmersión $Q \subset R$, determine la función producto de las que se suministran:

$$Z \to Q\colon f(x) = x/3$$
$$R \to R\colon g(x) = +\sqrt{x}$$

2.297.

Clasifique la función $y = \text{sen } x$, definida de R en R. Establezca su dominio y recorrido. Dibuje su gráfica cartesiana; también trace la representación de la función idéntica de R en R y, finalmente, dibuje la gráfica de la posible función inversa de la función seno.

Clasifique la «función» $R \to R\colon y = \text{arc sen } x$.

2.298.

Establecidas sobre el conjunto finito A, de potencia n, las combinaciones m-arias, demuéstrese, usando la complementación sobre A, que

$$\binom{n}{m} = \binom{n}{n-m}$$

2.299.

Justifíquese en álgebra conjuntista que

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

Sugerencia: Establézcase un conjunto finito A, de potencia n y, fijado un $a \in A$, realícese una partición entre las combinaciones que presentan ese elemento a y las que no lo presentan.

2.3

Ley de composición interna

2.31. Establecimiento

2.32. Grupoide

2.33. Subconjunto estable para una ley

2.34. Extensión de una ley en C a $C \times C$. Estabilidad frente a una relación de equivalencia

2.35. Conjunto y estructura. Acción de una operación sobre un conjunto: leyes de estructuración

2.351. *Elementos regulares. Ley de cancelación*
2.352. *Asociatividad*
2.353. *Semigrupo o monoide*
2.354. *Elemento neutro*
2.355. *Elementos simetrizables*
2.356. *Conmutatividad*

2.36. Un conjunto y dos leyes de composición interna: distributividad

2.37. Aplicabilidad. Automatismos y destrezas

2.3

Ley de composición interna

2.31. ESTABLECIMIENTO

Ley de composición interna u operación, definida en el conjunto C, es una *aplicación* del cartesiano $C \times C$ en C, tal que hace corresponder a cada par ordenado (a, b) del cartesiano una única imagen c del conjunto C.

Simbólicamente:

$$\left.\begin{array}{l} f \text{ es operación} \\ \text{en } C \end{array}\right\} \Leftrightarrow \forall (a, b) \in C \times C,\ \exists^* c \in C / f[(a, b)] = c$$

Es costumbre sustituir las típicas letras usadas en las aplicaciones (f, g, ...) por signos convencionales ($*$, $\perp$, ...). De este modo, escribiremos:

$$\left.\begin{array}{l} * \text{ es operación} \\ \text{en } C \end{array}\right\} \Leftrightarrow \forall (a, b) \in C \times C,\ \exists^* c \in C / *[(a, b)] = c$$

Aún más: se conviene en escribir el signo de la operación entre los elementos del par, que se llaman «operandos». Así:

$$C \times C \xrightarrow{*} C$$

$$(a, b) \xrightarrow{*} c$$

$$\boxed{a * b = c},$$

que se lee: «a operado b igual c».

2.32. GRUPOIDE

Así como las relaciones de equivalencia son agentes de clasificación y creadoras de entes matemáticos, así las leyes de composición son agentes de estructura, y son «los instrumentos para organizar y reglamentar el comportamiento» de los elementos de un conjunto.

Diremos que un *grupoide* lo constituye un conjunto C sobre el que al establecer una ley de composición, se le ha dotado de potencialidad de estructura.

El par $[C, *]$ representa un grupoide que puede alcanzar una determinada estructura.

2.33. SUBCONJUNTO ESTABLE PARA UNA LEY

Si sobre el conjunto C se ha establecido una ley de composición interna $*$, puede suceder que un $C_1 \subset C$ sea tal que, al operar dos elementos de él, el resultado siga perteneciendo a C_1. En tal caso se dice que C_1 es un subconjunto «estable» o «cerrado» para la operación $*$. Es decir:

$$\left.\begin{array}{c} C_1 \subset C \text{ es} \\ \text{estable para } * \end{array}\right\} \Leftrightarrow \forall (a, b) \in C_1 \times C_1,\ \exists^* c \in C_1 / a * b = c$$

Ejemplo

Los enteros múltiplos de 5 forman una parte estable para la adición en Z. En efecto:

$$5p + 5q = 5(p + q) = \dot{5}$$

2.34. EXTENSION DE UNA LEY EN C A $C \times C$. ESTABILIDAD FRENTE A UNA RELACION DE EQUIVALENCIA

Establecido el grupoide $[C, *]$, en el que la operación actúa así,

$$a * b = c,$$

puede pensarse en extender el formalismo de la ley a elementos del cartesiano $C \times C$, de tal modo que al operar dos pares, se compondrían de manera análoga a como lo hacen los elementos de C:

$$(a_1, b_1) * (a_2, b_2) = (c_1, c_2),$$

siendo:

$$c_1 = a_1 * a_2$$
$$c_2 = b_1 * b_2$$

Ejemplo

El producto de racionales podría establecerse por extensión del producto de enteros. Así:

en Z:

$$(+2) \times (-5) = (-10)$$
$$(+3) \times (+4) = (+12)$$

en Q:

$$\left\{\frac{+2}{+3}\right\} \times \left\{\frac{-5}{+4}\right\} = \left\{\frac{(+2) \times (-5)}{(+3) \times (+4)}\right\} = \left\{\frac{-10}{+12}\right\}$$

Considérese ahora un grupoide sobre el que se ha establecido una relación de equivalencia $\mathcal{R}$; es decir: $[C, *, \mathcal{R}]$.

Establezcamos un par de clases α y β, pertenecientes al conjunto cociente $C/\mathcal{R}$:

$$\alpha = \{a_1, a_2, \ldots, a_n\}$$
$$\beta = \{b_1, b_2, \ldots, b_n\}$$

Operemos un par de representantes de esas dos clases, por un lado,

$$a_1 * b_1 = c_1,$$

mientras que por otro, compongamos otro par cualquiera de ellos:

$$a_2 * b_2 = c_2$$

Si los resultados obtenidos c_1 y c_2 pertenecen a la misma clase γ del conjunto cociente $C/\mathcal{R}$, se dirá que la operación $*$ es estable frente a la relación de equivalencia $\mathcal{R}$.

En $[C, *, \mathcal{R}]$, $*$ es estable frente a $\mathcal{R}$ $\Leftrightarrow \forall a_i \in \alpha, \ \forall b_i \in \beta \ (\alpha \in C/\mathcal{R}, \ \beta \in C/\mathcal{R}), \ a_i * b_i = c_i/c_i \in \gamma, \ (\gamma \in C/\mathcal{R})$.

Lo anterior induce a establecer y justificar el siguiente

TEOREMA

Si la ley de composición $*$ de un grupoide dotado de una relación de equivalencia $\mathcal{R}$ es estable frente a ésta, induce en el conjunto cociente $C/\mathcal{R}$ una operación entre sus clases, $\bar{*}$.

En efecto: sean $a \in \{\alpha\}$ y $b \in \{\beta\}$.

Compongamos en C:

$$a * b = c$$

Establezcamos que $c \in \{\gamma\}$.

Como la ley $*$ es estable por hipótesis, la clase $\{\gamma\}$ es independiente de los operandos «a» y «b», escogidos de las clases $\{\alpha\}$ y $\{\beta\}$.

Ello establece, pues, una nueva ley entre clases, que simbolizamos

$$\boxed{\{\alpha\} \bar{*} \{\beta\} = \{\gamma\}}$$

Ejemplo

La multiplicación en Q es estable frente a la relación de equivalencia que define Q a partir de $Z \times Z^*$.

En efecto:

$$\left.\begin{array}{l} Q \ni \{\alpha\} = \left(\dfrac{a_1}{b_1}\right) \equiv \left(\dfrac{a_2}{b_2}\right) \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1 \\ Q \ni \{\beta\} = \left(\dfrac{c_1}{d_1}\right) \equiv \left(\dfrac{c_2}{d_2}\right) \Leftrightarrow c_1 \cdot d_2 = c_2 \cdot d_1 \end{array}\right\} \times$$

$$a_1 \cdot b_2 \cdot c_1 \cdot d_2 = a_2 \cdot b_1 \cdot c_2 \cdot d_1$$

$$\left\{\frac{a_1 \cdot c_1}{b_1 \cdot d_1}\right\} = \left\{\frac{a_2 \cdot c_2}{b_2 \cdot d_2}\right\}$$

$$\left\{\frac{a_1}{b_1}\right\} \times \left\{\frac{c_1}{d_1}\right\} = \left\{\frac{a_2}{b_2}\right\} \times \left\{\frac{c_2}{d_2}\right\}$$

Resultado, pues, independiente de los representantes de las clases, escogidos para operandos.

2.35. CONJUNTO Y ESTRUCTURA. ACCION DE UNA OPERACION SOBRE UN CONJUNTO: LEYES DE ESTRUCTURACION

Cuando sobre un conjunto C se establece una ley de composición interna, ésta le confiere una determinada estructura; pero —entiéndase bien— es un error tan extendido como lamentable entender que el conjunto C con la ley $*$ ES esta o aquella estructura. Citamos a Godement, que no duda en calificar este uso del verbo SER de «estupidez evidente».

2.351. Elementos regulares. Ley de cancelación

Establecido el grupoide $[C, *]$, considérese un $a \in C$, un $b \in C$, tal que $a = b$, y un $c \in C$.

Es obvio que

$$a = b \Rightarrow c * a = c * b$$

Sin embargo, no se puede asegurar que el recíproco sea siempre cierto:

Ejemplo

En $[Z, \times]$

$$(+7) \times 0 = (+5) \times 0 \not\Rightarrow (+7) = (+5)$$

Cuando se puede establecer que

$$\boxed{c * a = c * b \Rightarrow a = b} \quad \text{ó} \quad \boxed{a * c = b * c \Rightarrow a = b}$$

se dice que

c es elemento regular por la izquierda ó *c es elemento regular por la derecha,*

llamándole simplemente *regular*, si lo es por la izquierda y por la derecha.

Si todos los elementos de C son regulares para $*$, el grupoide $[C, *]$ goza de la ley cancelativa o de *simplificación*; es decir:

$$\forall a \in C,\ \forall b \in C,\ \forall c \in C$$
$$a * c = b * c \Rightarrow a = b$$

Ejemplo

En $[Z, +]$

$$(+4) + (x) = (+4) + (y) \Rightarrow (x) = (y)$$

2.352. Asociatividad

El grupoide $[C, *]$ goza de la propiedad asociativa, si

$$\forall a \in C,\ \forall b \in C,\ \forall c \in C,$$

$$\boxed{a * (b * c) = (a * b) * c = a * b * c}$$

Conviene hacer notar que la unicidad operativa se extiende a n operandos, sin más hipótesis que la expresada, y utilizando la recurrencia sobre n. O sea:

Estableciendo el grupoide $[A, *]$, $\forall a_i \in A$,

$$a_1 * \cdots * a_n = (a_1 * \cdots * a_p) * (a_{p+1} * \cdots * a_n) \qquad (1 \leq p \leq n)$$

2.353. Semigrupo o monoide

Si sobre un conjunto C se ha establecido una ley de composición interna $*$ asociativa, se dice que el grupoide $[C, *]$ ha sido dotado de estructura de *semigrupo* o *monoide*.

Ejemplo

$[N, +]$ alcanza la estructura de SEMIGRUPO aditivo.

2.354. Elemento neutro

Establecido el grupoide $[C, *]$, se dice que $\varepsilon \in C$ es elemento neutro si al componer cualquier elemento $a \in C$ con él, por la izquierda o por la derecha, el resultado es el propio elemento a. Es decir:

$$\left.\begin{array}{c}\varepsilon \text{ es elemento neutro} \\ \text{de } [C, *]\end{array}\right\} \Leftrightarrow \forall a \in C,\ \exists^* \varepsilon \in C / a * \varepsilon = \varepsilon * a = a$$

Ejemplo

$\{0\}$ es el neutro de $[Z, +]$
$\{+1\}$ es el neutro de $[Z, \times]$

Adviértase que en la definición apuntada aparece implícito el siguiente

TEOREMA

Si $[C, *]$ posee elemento neutro, éste es único.

Demostración:

Método por reducción al absurdo.

Admítase como hipótesis la negación de la tesis, es decir: el neutro no es único, o lo que es lo mismo: existen $\varepsilon_1 \neq \varepsilon_2$ neutros en $[C, *]$.

A_1) Por la naturaleza de neutro de ε_1:

$$\forall a \in C,\ \varepsilon_1 * a = a * \varepsilon_1 = a$$

B_1) Por la naturaleza de neutro de ε_2:

$$\forall a \in C,\ \varepsilon_2 * a = a * \varepsilon_2 = a$$

$A_2)$ Si $a \equiv \varepsilon_2$

$B_2)$ Si $a \equiv \varepsilon_1$

$$\left.\begin{array}{l} \varepsilon_1 * \varepsilon_2 = \varepsilon_2 * \varepsilon_1 = \varepsilon_2 \\ \varepsilon_2 * \varepsilon_1 = \varepsilon_1 * \varepsilon_2 = \varepsilon_1 \end{array}\right\} \varepsilon_2 = \varepsilon_1$$

Resultado contrario a la hipótesis establecida; es decir: la afirmación de la tesis es correcta.

2.355. Elementos simetrizables

Sea el grupoide $[C, *]$ que posee elemento neutro ε. Sea un $a \in C$.

Llamamos simétrico por la izquierda de a a un $a'' \in C / a'' * a = \varepsilon$

Definimos simétrico por la derecha de a, a un $a''' \in C / a * a''' = \varepsilon$

Simplemente se denominará simétrico de a a un

$$a' \in C / a' * a' = a * a' = \varepsilon$$

Se dice que un $a \in C$ es simetrizable si $\exists^* a' \in C$, simétrico de él.

NOTA. Adviértase que la distinción entre dextro y levo-simetrización carece de sentido en el caso —frecuente— de que la ley $*$ sea conmutativa.

TEOREMA. La condición necesaria y suficiente para que un elemento a de un grupoide asociativo con elemento neutro sea simetrizable es que posea simétrico a la izquierda y simétrico a la derecha, y que éstos coincidan; es decir: que tenga simétrico único.

Demostración:

Método por reducción al absurdo.

Admítase como hipótesis la negación de la tesis, es decir: el simétrico de a no es único, o lo que es lo mismo: existen $a'' \neq a'''/$

$$a * a'' = a'' * a = \varepsilon \qquad [1]$$
$$a * a''' = a''' * a = \varepsilon \qquad [2]$$

— Componiendo por la izquierda en [2] con a''

$$a'' * (a * a''') = a'' * \varepsilon$$

— Usando la asociatividad en el primer miembro y la naturaleza de neutro en el segundo,

$$(a'' * a) * a''' = a''$$

— Según [1],

$$\varepsilon * a''' = a''$$

— Por la naturaleza de neutro

$$a''' = a''$$

resultado contrario a la hipótesis establecida; es decir, la afirmación de la tesis es correcta.

TEOREMA. Si un $a \in C$ es simetrizable con $*$, su simétrico a' también lo es, siendo precisamente su simétrico a.

En realidad, este teorema no es más que un corolario del anterior, pues queda justificado con la relación involutiva de la simetrización:

$$a * a' = a' * a = \varepsilon,$$

o lo que es igual:

$$(a')' = a$$

TEOREMA. Si a y b son dos elementos simetrizables (no simétricos entre sí) de un semigrupo con elemento neutro, y $a * b = c$, el resultado c también es simetrizable, siendo su simétrico precisamente el compuesto de los simétricos de los operandos, cambiados de orden.

Simbólicamente

$$\left.\begin{array}{ll} (1) & a * a' = a' * a = \varepsilon \\ (2) & b * b' = b' * b = \varepsilon \\ (3) & a * b = c \\ (4) & c * c' = c' * c = \varepsilon \end{array}\right\} \Rightarrow c' = b' * a'$$

Demostración:

A dos columnas realizaremos la simetrización, a izquierda y a derecha.

A) Compongamos (3) por la izquierda (derecha) con $(b' * a')$

$$(b' * a') * (a * b) = (b' * a') * c \qquad (a * b) * (b' * a') = c * (b' * a')$$

B) Asociatividad

$$b' * (a' * a) * b = (b' * a') * c \qquad a * (b * b') * a' = c * (b' * a')$$

C) Por la naturaleza de los elementos simétricos

$$b' * \varepsilon * b = (b' * a') * c \qquad a * \varepsilon * a' = c * (b' * a')$$

D) Por la naturaleza de neutro

$$b' * b = (b' * a') * c \quad ; \quad a * a' = c * (b' * a')$$

E) Por la naturaleza de los elementos simétricos

$$\underline{\varepsilon = (b' * a') * c} \quad ; \quad \underline{\varepsilon = c * (b' * a')}$$

$$\boxed{c' = b' * a'}$$

Nomenclatura y formulación específicas: notación exponencial

Si se trata de leyes aditivas, los elementos simétricos se denominan *opuestos*; y —si como es normal— el neutro de estas leyes se le representa por 0, la simetrización de una ley aditiva toma la forma

$$a + (-a) = (-a) + a = 0$$

En las leyes de tipo multiplicativo los pares de elementos simétricos reciben el nombre de *inversos*; si la operación se denota por $\times$, la simetrización de una ley de este tipo se describe así:

$$a \times a^{-1} = a^{-1} \times a = 1$$

El elemento neutro de esta clase de operaciones recibe el nombre de elemento *unidad.*

Si la ley asociativa de un grupoide compone un elemento consigo mismo, se conviene en esta representación

$$a * a = a^2,$$

y también

$$(a * a) * a = a^2 * a = a^3.$$

Generalizando,

$$a^{n-1} * a = a^n.$$

Bien fáciles de justificar son las conocidas simbolizaciones asociativas

$$a^m * a^n = a^{m+n}$$

$$(a^m)^n = a^{m \cdot n}.$$

Generalizando del todo el convenio de escritura, y asignando

$$a = a^1 \quad \text{y} \quad a^0 = 1,$$

se simboliza

$$(a^{-1})^p = a^{-p} \qquad \text{(Véase teorema anterior.)}$$

2.356. Conmutatividad

Establecido el grupoide $[C, *]$, se dice que goza de la propiedad conmutativa o que es «abeliano», si

$$\forall a \in C,\ \forall b \in C,$$
$$a * b = b * a$$

TEOREMA. Si el grupoide $[C, *]$ alcanza la estructura de semigrupo abeliano (asociativo y conmutativo), el resultado de componer n elementos de C es independiente del orden de los operandos.

En efecto: se puede conseguir cualquier orden prefijado de operandos, si se consigue demostrar que son permutables dos operandos consecutivos a_k y a_{k+1}.

> Procedemos a realizar la demostración en notación aditiva, indicando al lector-estudiante la conveniencia de que desarrollara el teorema, por su cuenta, con la simbolización multiplicativa que le indicamos:
>
> $\prod_{i \in I} a_i = a_1 \cdot, \ldots, \cdot a_k \cdot a_{k+1} \cdot, \ldots, \cdot a_n$

0) Se establece: (y por asociatividad)

$$\Sigma\, a_i = a_1 + \cdots + a_k + a_{k+1} + \cdots + a_n.$$

$$\sum_{i \in I} a^i = \sum_{i=1}^{i=k-1} a_i + a_k + a_{k+1} + \sum_{i=k+2}^{i=n} a_i$$

1) Por asociatividad

$$\sum_{i \in I} a_i = \sum_{i=1}^{i=k-1} a_i + (a_k + a_{k+1}) + \sum_{i=k+2}^{i=n} a_i$$

2) Por conmutatividad

$$\sum_{i \in I} a_i = \sum_{i=1}^{i=k-1} a_i + (a_{k+1} + a_k) + \sum_{i=k+2}^{i=n} a_i$$

3) Por asociatividad

$$\sum_{i \in I} a_i = \sum_{i=1}^{i=k-1} a_i + a_{k+1} + a_k + \sum_{i=k+2}^{i=n} a_i$$

4) Es decir:

$$\sum_{i \in I} a_i = a_1 + \cdots + a_{k+1} + a_k + \cdots + a_n$$

2.36. UN CONJUNTO Y DOS LEYES DE COMPOSICION INTERNA: DISTRIBUTIVIDAD

Considérese que sobre el conjunto C se han establecido las dos operaciones $*$ y $\perp$.

Se dirá que $\perp$ es distributiva, por la izquierda, respecto a $*$, si sucede que $\forall a \in c$, $\forall b \in C$, $\forall c \in C$,

$$a \perp (b * c) = (a \perp b) * (a \perp c). \qquad [1]$$

Análogamente se entenderá que $\perp$ es distributiva por la derecha, respecto de $*$, si sucede que:

$$(b * c) \perp a = (b \perp a) * (c \perp \text{a}); \qquad [2]$$

siendo el caso más interesante y frecuente la distributividad bilátera; entonces —al cumplirse [1] y [2]— se dirá simplemente que la operación $\perp$ es distributiva respecto de la $*$.

Ejemplo

La $\times$ es distributiva respecto de la $+$ en $[N, +, \times]$.

En Z:

$$(a) \cdot [(b) + (c)] = (a \cdot b) + (a \cdot c)$$

La $\times$ es distributiva respecto de la adición en $[Q, +, \times]$.

NOTA. Adviértase lo improcedente de decir que tal o cual estructura bioperacional es distributiva. Ha de especificarse la ley que es agente de la distribución, respecto de la otra.

Ejemplo

Algunas estructuras simples, tal es el «álgebra de Boole», gozan de distributividad dual. Por ejemplo: en el álgebra de Boole concreta de los conjuntos, sucede

$$A) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$B) \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

TEOREMA. Si la ley distributiva lo es respecto a una operación asociativa, la distributividad se extiende a los compuestos aditivos (los resultados de la ley asociativa).

Ejercicio-ejemplo.

Dejamos al cuidado del lector que pruebe este sencillo teorema, sobre $[Z, +, \times]$

$$(a + b) \cdot (c + d) = (a \cdot c) + (b \cdot c) + (a \cdot d) + (b \cdot d)$$

2.37. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

Se proponen a continuación algunos instrumentos de aprendizaje que suponemos útiles, intercalados en el estudio teórico del tema:

2.371.

Justifíquese si $P \subset Z$ es estable para la ley $+$, en el que

$$P = \{\text{números primos}\}$$

2.372.

En Q se establece la ley $x * y = \frac{x + y}{2}$. Investíguese si el grupoide $[Q, *]$ puede alcanzar la estructura de semigrupo abeliano.

2.373.

Sobre el conjunto $M = \{1, 2, 5\}$ se establece la ley $x * y = r$, siendo $x^y = 3k + r$. Complete la tabla de la operación (convenio: tome como primeros operandos los expresados en la primera fila, y como segundos, los escritos en la primera columna)

*	1	2	5
1			2
2			
5			1

2.374.

En N es establece la ley $x * y = x + y + x \cdot y$.
Investíguese si es o no asociativa.

2.375.

En Q se establece la ley $x * y = x + \frac{1}{y}(y \neq 0)$. Pruébese si el grupoide $[Q, *]$ alcanza la estructura de semigrupo.

2.376.

Sobre el conjunto Z se establece la relación de equivalencia $\mathcal{R}$ = «dar el mismo resto al dividir por 3».

a) Determínese el conjunto cociente $Z/\mathcal{R}$.

b) Véase si la adición en Z es estable frente a la relación de equivalencia establecida.

2.377.

En el conjunto de los números naturales se definen las operaciones siguientes:

$$a * b = a + 2b$$
$$a \perp b = 2ab$$

Verifíquese si la segunda es distributiva respecto de la primera.

2.378.

Dado el conjunto $A = \{x/3k = x;\ k \in Z\}$,

a) justifique si la adición en A es ley de composición interna;

b) pruebe si la multiplicación en A es operación.

2.379.

Se establece el conjunto Z^+ y sobre él las dos leyes

$$a * b = \text{m.c.d. } (a, b)$$
$$a \perp b = \text{m.c.m. } (a, b)$$

a) investigue la posible conmutatividad de la primera;

b) justifique la asociatividad de la segunda.

2.37.10.

Demuestre con los establecimientos anteriores que en $[Z^+, \times, *]$ la multiplicación es distributiva respecto de $*$.

2.4

Grupos

2.41. Establecimiento de la estructura de grupo

2.42. Grupos finitos y no finitos

2.43. Creación de grupos: simetrización de semigrupos

2.431. *Necesidad histórica: las «imposibles operaciones inversas»*
2.432. *Simetrización*

2.4321. Condiciones del semigrupo a simetrizar para producir el grupo
2.4322. Simetrización
2.4323. El semigrupo simetrizado «sumergido» en el grupo creado

2.44. Un grupo histórico: el grupo simétrico de *n* variables G_n

2.441. *Permutación. Sustitución. Ciclo. Transposición*
2.442. *El grupo de las sustituciones $G(A)$*

2.4421. Ley de composición interna en $G(A)$
2.4422. Estructuración de $G(A)$

2.443. *Las sustituciones como producto de transposiciones*
2.444. *Paridad de una sustitución. Inversión en una permutación. Signatura de una sustitución*

2.45. Grupos monógenos: grupos cíclicos; generadores

2.46. Subgrupos

2.461. *Establecimiento*
2.462. *Teorema*

2.47. El grupo de las transformaciones

2.471. *Ley de composición externa: operadores*
2.472. *Operadores con estructura de grupo*
2.473. *El grupo de las transformaciones*
2.474. *Orbita de* a *generada por un grupo de operadores*

2.48. Conjunto cociente, módulo un subgrupo

2.481. *Clases adjuntas*
2.482. *Teorema*
2.483. *Indice de H en G. Teorema de Lagrange*
2.484. *Subgrupos normales, invariantes o distinguidos*
2.485. *Grupo cociente del grupo G respecto del subgrupo invariante H*

2.49. Aplicabilidad. Automatismos y destrezas

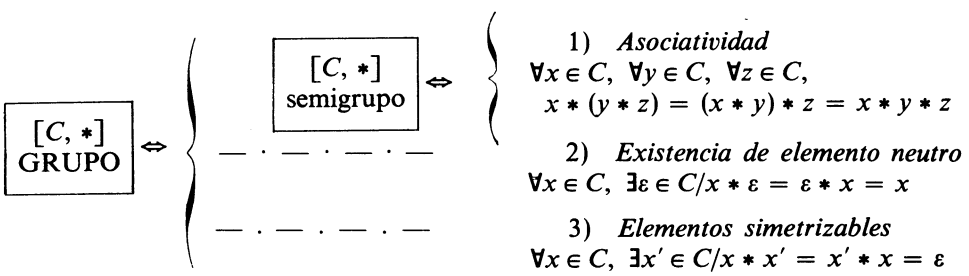
2.4

Grupos

2.41. ESTABLECIMIENTO DE LA ESTRUCTURA DE GRUPO

Siendo el conjunto $C \neq \phi$ y una ley de composición interna $*$, se dice que el grupoide $[C, *]$ alcanza la estructura de *grupo* si funciona como un semigrupo con elemento neutro en el que todos sus elementos son simetrizables.

Esquemáticamente:



Si, como es frecuente, además

4) *Conmutatividad*
$\forall x \in C,\ \forall y \in C,\ x * y = y * x,$

entonces se dice que $[C, *]$ tiene estructura de *grupo abeliano*.

Ejercicio-Ejemplo

$[Z, +]$ tiene estructura de grupo abeliano. Desarróllese.

Consecuencias inmediatas de la axiomática expuesta son los cinco teoremas elementales siguientes, de los que solamente demostraremos el último de ellos

dejando a la consciente labor del estudiante la sencilla justificación de los otros cuatro, en trabajo de consulta a anteriores desarrollos.

TEOREMA. El formalismo asociativo, axiomatizado para tres elementos de un grupo abeliano es extensible a la composición de n operandos.

TEOREMA. El elemento neutro de un grupo es único.

TEOREMA. Para cada elemento de un grupo existe un solo simétrico.

TEOREMA. Todo grupo goza de la ley cancelativa, por ser todos sus elementos regulares.

TEOREMA. En el grupo $[C, *]$ existen un solo x y un solo y que satisfacen las ecuaciones

0) $\boxed{a * x = b}$ e $\boxed{y * a = b}$

1) Se compone por la izquierda (por la derecha) con el simétrico de a:

$$a' * (a * x) = a' * b \qquad (y * a) * a' = b * a'$$

2) Por asociatividad

$$(a' * a) * x = a' * b \qquad y * (a * a') = b * a'$$

3) Por la naturaleza de los elementos simétricos:

$$\varepsilon * x = a' * b \qquad y * \varepsilon = b * a'$$

4) Por la naturaleza del elemento neutro:

$$\boxed{x = a' * b} \qquad \boxed{y = b * a'}$$

COROLARIO: Si el grupo es abeliano, evidentemente

$$\boxed{x = y}$$

2.42. GRUPOS FINITOS Y NO FINITOS

El grupo $[C, *]$ es un grupo finito, si C es un conjunto finito.
En este caso, se dice que el *orden del grupo* es c, si $\text{card}(C) = c$.

Ejemplo

El conjunto de las raíces en $\mathbb{C}$ de la ecuación

$$x^4 - 1 = 0$$

forman un grupo multiplicativo abeliano de orden 4. En efecto, el conjunto de sus raíces es

$$X = \{1, -1, i, -i\}$$

(El desarrollo de este ejemplo es objeto de ejercicio en el epígrafe final del capítulo.)

Ejemplo

Es clásico el conjunto de isometrías planas que transforman un determinado triángulo equilátero en sí mismo.

Es un grupo de orden 6, ya que son seis los movimientos que integran el conjunto isométrico:

$$\mathcal{T} = \{G_0, G_{120^\circ}, G_{-120^\circ}, S_A, S_B, S_C\},$$

símbolos referibles a la aplicación 2.492, donde se desarrollará el ejercicio.

Si el conjunto que es sustrato de la estructura de grupo tiene infinitos elementos, se tiene un grupo no finito.

Ejemplo

$[Z, +]$ presenta estructura de grupo abeliano no finito.

Su desarrollo es objeto de ejercicio en la aplicación 2.49.10.

Ejemplo

$[Q - \{0\}, \times]$ tiene estructura de grupo abeliano no finito.

Igualmente, se propone al lector su estudio en el ejercicio 2.49.10.

2.43. CREACION DE GRUPOS: SIMETRIZACION DE SEMIGRUPOS

La estructura de grupo es sumamente rica y fecunda, y ello por dos razones:

Primera: en todo grupo $[C, *]$ puede establecerse una ley, que llamaremos «inversa» de $*$ (y que simbolizaremos $*'$), del siguiente modo:

$$\forall a \in C, \quad \forall b \in C, \quad a *' b = b' * a$$

(Como siempre b y b' simbolizan elementos simétricos.)

Ejemplo

En el grupo $[Z, +]$ se establece la ley «diferencia» así:

$$a - b = (-b) + a$$

$$(+3) - (+7) = (-7) + (+3) = (-4)$$

Ejemplo

En el grupo $[Q - \{0\}, \times]$ se establece la ley «división» así:

$$\{a\} : \{b\} = \{1/b\} \times \{a\} = \{a/b\}$$
$$\{2/3\} : \{7/5\} = \{5/7\} \times \{2/3\} = \{10/21\}$$

Segunda: los elementos de un grupo tienen naturaleza de *operadores*, concepto capital en estructuras más ricas, con leyes de composición externas.

Advertencia al lector

Es lógico que esta segunda razón (la de mayor entidad de ambas) presente dificultad en primera lectura.

Para su plena comprensión, vuelva a ella, tras el estudio del epígrafe 2.472.

2.431. Necesidad histórica: las «imposibles operaciones inversas»

En el semigrupo aditivo de los naturales (con el 0), $[N \cup \{0\}, +]$, no siempre tiene solución la ecuación

(1) $$a + x = b.$$

Si $b < a$, no existe ningún $x \in N$ que satisfaga la igualdad establecida.

En el semigrupo multiplicativo de los enteros $[Z, \times]$, la ecuación

(2) $$a \cdot x = b,$$

solamente tiene solución, si

$$b = \dot{a}$$

En general, en el semigrupo $[C, *]$, la ecuación

$$a * x = b,$$

solamente tendrá solución en el caso excepcional, en que el simétrico de a pertenezca a C, caso absolutamente particular, ya que en la estructura de semigrupo no todos (o ninguno) de los elementos son simetrizables.

Para obviar la dificultad que presenta la resolución de la ecuación (1) en N, se creó un grupo —el de los enteros dotados de la adición $[Z, +]$— en el que quedaba «sumergido» el

Con el fin de dar solución a la ecuación (2), aun cuando $b \neq \dot{a}$, se creó un grupo —el de los racionales privados de la clase $\{0\}$, dotados de la multiplicación, $[Q - \{0\}, \times]$— en el

semigrupo aditivo de los naturales.

En este grupo ya es posible escribir

$$x = b - a,$$

aun cuando $b < a$.

Se «inventaba» así la «sustracción», ley «inversa» de la adición.

que quedaba «sumergido» el semigrupo multiplicativo de los enteros.

En este grupo ya es posible escribir siempre

$$x = b/a$$

Con ello, quedaba establecida la «división», como ley «inversa» de la multiplicación.

En ambos casos el proceso de creación del grupo, a partir del semigrupo, es análogo. Ello permite pensar en un proceso, del todo general, de construcción de grupos, que —en efecto— está elaborado y se denomina

2.432. Simetrización

2.4321. *Condiciones del semigrupo a simetrizar para producir el grupo*

Tal vez se haya advertido que en los ejemplos paralelos, anteriormente desarrollados, se trataba en ambos casos de estructuras iniciales de semigrupos abelianos, cuyos elementos eran todos regulares.

En efecto: las dos condiciones para poder simetrizar un semigrupo son éstas:

1.ª) el semigrupo a simetrizar ha de ser conmutativo;

2.ª) el semigrupo a simetrizar ha de poseer la ley de cancelación.

NOTA AL LECTOR. De propósito, en los últimos párrafos se han usado sinónimos y expresiones equivalentes, que no pretenden hacer la lectura molesta ni la construcción artificiosa.

Bueno será que con ello se consigan los automatismos de una lectura ágil del lenguaje matemático, propio de los elementos de álgebra que nos ocupan.

2.4322. *Simetrización*

HIPOTESIS

Establecimientos:

E_1) $[C, *]$ tiene estructura de semigrupo abeliano cancelativo

E_2) Se construye el cartesiano $C \times C$

E_3) Se crea una relación de equivalencia $\mathfrak{R}$, sobre $C \times C$

$E_{3.1}$) *Establecimiento de* $\mathfrak{R}$ (notación: $\equiv$)

$$(a, b) \in C \times C, \qquad (c, d) \in C \times C$$

$$(a, b) \equiv (c, d) \Leftrightarrow a * d = b * c$$

$E_{3.2}$) *Análisis de* $\mathfrak{R}$: Esta relación es de equivalencia. En efecto:

a) Reflexividad

$$(a, b) \equiv (a, b) \Leftrightarrow a * b = b * a$$

($[C, *]$ es abeliano)

b) Simetría

$$(a, b) \equiv (c, d) \Rightarrow (c, d) \equiv (a, b)$$
$$\Updownarrow$$
$$a * d = b * c$$
$$\Downarrow \qquad ([C, *] \text{ es abeliano})$$
$$a * d = c * b$$
$$\Downarrow$$
$$c * b = a * d \Leftrightarrow (c, d) \equiv (a, b)$$

c) Transitividad

$$\left.\begin{array}{l}(a, b) \equiv (c, d)\\ (c, d) \equiv (e, f)\end{array}\right\} \Rightarrow (a, b) \equiv (e, f)$$

$$\left.\begin{array}{l}(a, b) \equiv (c, d) \Leftrightarrow a * d = b * c\\ (c, d) \equiv (e, f) \Leftrightarrow c * f = d * e\end{array}\right\} \ *$$
$$(a * d) * (c * f) = (b * c) * (d * e)$$
$$\Downarrow \text{ Asociatividad}$$
$$a * d * c * f = b * c * d * e$$
$$\Downarrow \text{ Cancelación}$$
$$a * f = b * e$$
$$\Updownarrow$$
$$(a, b) \equiv (e, f)$$

$E_{3.3}$) *Acción de* $\mathfrak{R}$ *sobre* $C \times C$

$\mathfrak{R}$ clasifica y parte a $C \times C$ en clases de equivalencia, que son elementos del conjunto-cociente

$$\mathbf{C} = C \times C/\mathfrak{R} = \{\{\alpha\}, \{\beta\}, \{\gamma\}, \ldots\}$$
$$\{\alpha\} = \{(a_1, b_1) \equiv (a_2, b_2) \ldots\}$$
$$\{\beta\} = \{(c_1, d_1) \equiv (c_2, d_2) \ldots\}$$

E_4) Al ser estable la ley $*$, frente a la relación de equivalencia $\mathfrak{R}$ que define $\mathbf{C}$ a partir de $C \times C$, induce una ley de composición interna $\bar{*}$ entre las clases de $\mathbf{C}$.

Indicación: Es muy probable que sea oportuno consultar ahora la sección 2.34 del capítulo anterior.

$$\forall\{(a, b)\} \in C \times C/\mathfrak{R}, \quad \forall\{(c, d)\} \in C \times C/\mathfrak{R},$$
$$\{(a, b)\} \bar{*} \{(c, d)\} = \{(a * c, b * d)\}$$

TESIS

$[C \times C/\mathfrak{R}, \bar{*}]$ tiene estructura de grupo abeliano.

DEMOSTRACION

D_0) *Uniformidad*: La ley $\bar{*}$ es cerrada en $\mathbb{C} \equiv C \times C/\mathfrak{R}$. Es decir, el resultado pertenece a $\mathbb{C}$, y es único.
Justificación: La ley $*$ lo es en C y se ha establecido que es estable frente a la relación $\mathfrak{R}$.

D_1) *Asociatividad*:

$$\{(a, b)\} \bar{*} [\{(c, d)\} \bar{*} \{(e, f)\}] = [\{(a, b)\} \bar{*} \{(c, d)\}] \bar{*} \{(e, f)\}$$

Justificación: Basta operar ambos miembros, como lo hacemos, a dos columnas:

$$\begin{array}{l|l} \{(a, b)\} \bar{*} [\{(c, d)\} \bar{*} \{(e, f)\}] = & [\{(a, b)\} \bar{*} \{(c, d)\}] \bar{*} \{(e, f)\} = \\ = \{(a, b)\} \bar{*} [\{(c, * e, d * f)\}] = & = [\{(a * c, b * d)\}] \bar{*} \{(e, f)\} = \\ = \{(a * c * e \quad , \quad b * d * f)\} & = \{(a * c * e \quad , \quad b * d * f)\} \end{array}$$

D_2) *Existencia de elemento neutro*:

$$\{(a, b)\} \bar{*} \{(n, n)\} = \{(n, n)\} \bar{*} \{(a, b)\} = \{(a, b)\}$$

Justificación: $a * (n * b) = b * (n * a)$

$$\Downarrow$$

$$\{(a, b)\} = \{(n * a \quad , \quad n * b)\} = \{(n, n)\} \bar{*} \{(a, b)\}$$

D_3) *Elementos simetrizables*:

$$\{(a, b)\} \bar{*} \{(b, a)\} = \{(a * b, b * a)\} = \{(a * b, a * b)\} \equiv \{(n, n)\}$$

D_4) *Conmutatividad*

$$\{(a, b)\} \bar{*} \{(c, d)\} = \{(c, d)\} \bar{*} \{(a, b)\}$$

En efecto:

$$\{(a, b)\} \bar{*} \{(c, d)\} = \{(a * c, b * d)\} = \{(c * a, d * b)\} = \{(c, d)\} \bar{*} \{(a, b)\}$$

2.4323. *El semigrupo simetrizado «sumergido» en el grupo creado*

Para establecer esta «captación» del semigrupo por el grupo creado, es necesario disponer antes de las nociones de *homomorfismo* y específicamente de *isomorfismo*, conceptos extremadamente importantes, que se desarrollarán en el capítulo siguiente. Allí surgirán suficientes ocasiones de referirnos a esta cuestión, a la que aquí se pone punto final.

2.44. UN GRUPO HISTORICO: EL GRUPO SIMETRICO DE n VARIABLES G_n

2.441. Permutación. Sustitución. Ciclo. Transposición

Se establece un conjunto finito ordenado, por ejemplo el $A = \{a_1, a_2, a_3\}$. Se denomina *permutación de A* a cada uno de los conjuntos-imagen producidos por todas las biyecciones posibles de A en A.

Desde los estudios elementales de combinatoria, se sabe que el número de las posibles biyecciones de A en A es $n!$, si el conjunto finito tiene n elementos.

En el ejemplo establecido será, pues, $3! = 6$; a saber:

$$(a_1, a_2, a_3);\ (a_2, a_3, a_1);\ (a_3, a_1, a_2);\ (a_1, a_3, a_2);\ (a_2, a_1, a_3);\ (a_3, a_2, a_1).$$

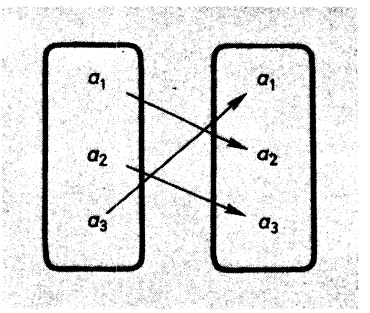
Sustitución

A cada una de las biyecciones establecidas se la denomina *sustitución*, y puede quedar simbolizada por un cuadro de elementos que disponga en línea inferior el conjunto original, y en la superior la permutación correspondiente. De esta manera:

$$S_1 = \begin{bmatrix} a_1, a_2, a_3 \\ a_1, a_2, a_3 \end{bmatrix};\quad S_2 = \begin{bmatrix} a_2, a_3, a_1 \\ a_1, a_2, a_3 \end{bmatrix};\quad S_3 = \begin{bmatrix} a_3, a_1, a_2 \\ a_1, a_2, a_3 \end{bmatrix};$$

$$S_4 = \begin{bmatrix} a_1, a_3, a_2 \\ a_1, a_2, a_3 \end{bmatrix};\quad S_5 = \begin{bmatrix} a_2, a_1, a_3 \\ a_1, a_2, a_3 \end{bmatrix};\quad S_6 = \begin{bmatrix} a_3, a_2, a_1 \\ a_1, a_2, a_3 \end{bmatrix}.$$

«Visualicemos», usando diagramas de Venn, por ejemplo, la sustitución S_2:



Ciclo: También denominada «sustitución circular» es la sustitución de n elementos, en la que cada imagen $f(a_k)$ coincide con el antecedente de la consecutiva: o sea $f(a_k) = a_{k+1}$, siendo $f(a_n) = a_1$.

Un esquema de ciclo es

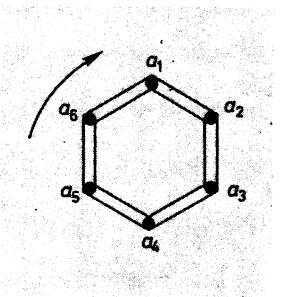
$$\begin{bmatrix} a_2, \ldots, a_{k+1}, & \ldots, a_1 \\ a_1, \ldots, a_k, a_{k+1}, & \ldots, a_n \end{bmatrix}$$

La S_2, antes establecida, es un ciclo.

Símil visual: Una imagen sumamente intuitiva de ciclo se consigue disponiendo en los n vértices de un polígono regular la permutación original, y asignando a cada elemento el que le sigue en la figura geométrica.

Por ejemplo: establecida la permutación principal $(a_1, a_2, a_3, a_4, a_5, a_6)$, un ciclo sería la sustitución

$$\begin{bmatrix} a_2, a_3, a_4, a_5, a_6, a_1 \\ a_1, a_2, a_3, a_4, a_5, a_6 \end{bmatrix}$$



Transposición es una sustitución en la que la permutación original y la permutación-imagen coinciden, a excepción de dos elementos, que forman un ciclo binario.

Ejemplo

$$\begin{bmatrix} a, & (c, & b,) & d, & e \\ a, & (b, & c,) & d, & e \end{bmatrix}$$

2.442. El grupo de las sustituciones $G(A)$

Definido el concepto de sustitución y establecido, así mismo, el conjunto de ellas en un conjunto A, vamos a crear una ley de composición interna, llamada «producto», que estructurará el conjunto de las sustituciones $G(A)$ en forma de grupo.

2.4421. *Ley de composición interna en* $G(A)$

$$\forall f \in G(A), \quad \forall g \in G(A), \quad \exists^* h \in G(A) \,/\, g \cdot f = h$$

Operatividad de la ley

Sea $A = \{a_1, a_2, a_3\}$

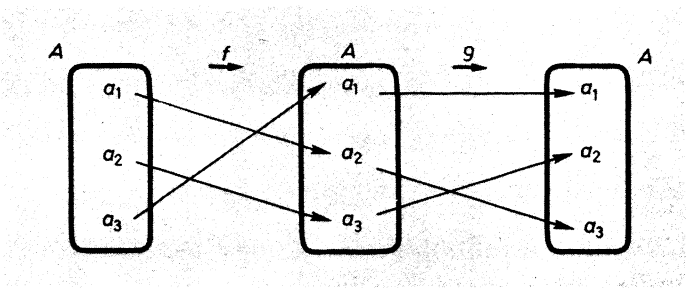
Considérense, de las 3! sustituciones de $G(A)$, estas dos:

$$f = \begin{bmatrix} a_2, a_3, a_1 \\ a_1, a_2, a_3 \end{bmatrix} \qquad g = \begin{bmatrix} a_1, a_3, a_2 \\ a_1, a_2, a_3 \end{bmatrix}$$

El producto de ambas, $g \cdot f = h$, se consigue aplicando a cada elemento de la permutación «principal» primero f; y luego, sobre la permutación-imagen —dada por f— se aplica g. De modo que:

$$h = g \cdot f = \begin{bmatrix} a_3, a_2, a_1 \\ a_1, a_2, a_3 \end{bmatrix}$$

Sensibilicemos el concepto con una interpretación gráfica:



$$\begin{array}{lll} f(a_1) = a_2 & f(a_2) = a_3 & f(a_3) = a_1 \\ g(a_2) = a_3 & g(a_3) = a_2 & g(a_1) = a_1 \\ \hline g[f(a_1)] = a_3 & g[f(a_2)] = a_2 & g[f(a_3)] = a_1 \\ g \cdot f(a_1) = a_3 & g \cdot f(a_2) = a_2 & g \cdot f(a_3) = a_1 \end{array}$$

$$h = g \cdot f = \begin{bmatrix} a_3, a_2, a_1 \\ a_1, a_2, a_3 \end{bmatrix}$$

2.4422. *Estructuración de $G(A)$*

La ley establecida, «producto», dota a $G(A)$ de estructura de grupo. En efecto:

I. *Uniformidad*: El producto de dos sustituciones de $G(A)$ producen otra sustitución de $G(A)$, además única.
(Adviértase que se definió la ley como aplicación $G(A) \times G(A) \dashrightarrow G(A)$.)

II. *Asociatividad*:

$$\forall f \in G(A),\ \forall g \in G(A),\ \forall h \in G(A),$$
$$h \cdot [g \cdot f] = [h \cdot g] \cdot f$$

(Efectivamente, ya que el producto de sustituciones es una composición de aplicaciones, operación que, en su lugar, se justificó como asociativa.)

III. *Existencia de elemento unidad*

$$\forall f \in G(A),\ \exists I \in G(A)/I \cdot f = f \cdot I = f$$

La sustitución denotada por I es la denominada «sustitución idéntica», representada por cualquiera cuyas dos permutaciones sean iguales

$$I = \begin{bmatrix} a_i, a_j, a_k \\ a_i, a_j, a_k \end{bmatrix}$$

(Basta operar para justificar el establecimiento.)

IV. *Elementos inversos*

$$\forall f \in G(A),\ \exists f^{-1} \in G(A) / f^{-1} \cdot f = f \cdot f^{-1} = I$$

(La comprobación es inmediata para cada elemento del grupo finito que nos ocupa.)

Expresando que, en general, el producto de sustituciones no es conmutativo, queda establecido (usando uno de orden 3) el grupo simétrico de n variables $[G_n(A), \times]$.

Galois, en 1832, estudiando este grupo, puso la primera piedra de la extensa y fecunda Teoría de Grupos.

2.443. Las sustituciones como producto de transposiciones

Existen tres proposiciones interesantes al respecto, que son éstas:

1.ª Toda sustitución se puede descomponer en un producto finito de ciclos disjuntos;

2.ª Todo ciclo se puede establecer como producto de transposiciones;

3.ª Toda sustitución es un producto de transposiciones.

Si las dos primeras se toman como teoremas (fácilmente demostrables por recurrencia), entonces la 3.ª es un evidente corolario de ambas.

Sin embargo, por considerarlo más general —a título de ejemplo— nosotros intentaremos demostrar, también por recurrencia, la 3.ª proposición, como teorema independiente de los dos anteriores.

(Si es oportuno, bien puede el lector interesado consultar y ejercitarse —según el procedimiento indicado— en demostrar las dos proposiciones primeras, y presentar la 3.ª como corolario de ellas.)

Así, pues,

TEOREMA. Toda sustitución $f \in G_n(A)$ es igual a un producto de transposiciones.

Demostrémoslo por recurrencia:

1.º Para $n = 1$ y $n = 2$ la comprobación es obvia:

$$n = 1\colon A = \{a\} \quad ; \quad G_1 = \left\{ \begin{pmatrix} a \\ a \end{pmatrix} \right\}$$

$$n = 2\colon A = \{a_1, a_2\} \quad ; \quad G_2 = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}, \begin{pmatrix} a_2 & a_1 \\ a_1 & a_2 \end{pmatrix} \right\}$$

2.º Admitamos que la tesis es cierta para el grupo $G_{n-1}(A)$ y sea f_1 una sustitución cualquiera del grupo citado.

3.º Justifiquemos que el teorema se cumple en el grupo $G_n(A)$. Sea f una sustitución cualquiera del grupo $G_n(A)$:

$$f = \begin{bmatrix} \dots a_j \dots \\ \dots a_k \dots \end{bmatrix}$$

Pueden suceder dos cosas:

A) que en f haya un $a_i / f(a_i) = a_i$.

Entonces, considerando la restricción de f a los restantes elementos, prescindiendo del $\begin{pmatrix} a_i \\ a_i \end{pmatrix}$, se obtiene una sustitución f_1 del grupo $G_{n-1}(A)$, que —según 2.º— se puede descomponer en producto de transposiciones.

De modo que asociando a toda $f_1 \in G_{n-1}(A)$ una transposición del $G_n(A)$, que deja invariante a_i, queda justificado el grupo $G_n(A)$, como producto de transposiciones;

B) que en f no haya ningún a_i cuya imagen sea él mismo.

Establecemos que $f(a_i) = a_j$, y que la transposición $t \in G_n(A)$, es la que cambia a_i y a_j:

$$t = \begin{bmatrix} \dots & \begin{pmatrix} a_j & a_i \\ a_i & a_j \end{pmatrix} & \dots \end{bmatrix}$$

La sustitución producto $g = t \cdot f$ pertenece a $G_n(A)$, y se puede considerar como la asociada a una $g_1 \in G_{n-1}(A)$, con la transposición escrita.

En fin: que hemos conseguido también en este caso la misma situación que en *A*), con lo que el teorema queda terminado.

2.444. Paridad de una sustitución. Inversión en una permutación. Signatura de una sustitución

Establecida una sustitución f del grupo $G_n(A)$, simbolizando la permutación original por P_1 y la permutación imagen por P_2

$$f = \begin{bmatrix} P_2 \\ P_1 \end{bmatrix},$$

siendo a_i y a_k dos elementos cualesquiera de P_1, diremos que el par de imágenes $f(a_i)$ y $f(a_k)$ son una inversión de la permutación P_2, si el orden de los antecedentes es distinto del orden de sus imágenes.

Ejemplo

Sobre el finito $A = \{a_1, a_2, a_3\}$, la permutación (a_3, a_1, a_2) de la sustitución

$$f = \begin{bmatrix} a_3, a_1, a_2 \\ a_1, a_2, a_3 \end{bmatrix},$$

presenta las inversiones (a_3, a_1) y (a_3, a_2).

Se dice que una sustitución es *par* si el número de inversiones de su permutación imagen es par; si es impar el número de inversiones que presenta supermutación imagen, consecuentemente, se denomina sustitución *impar*.

Ejemplo

Establezcamos un $A = \{1, 2, 3, 4, 5\}$ y una $f \in G(A)$, una $g \in G(A)$ y una $h \in G(A)$,

$$f = \begin{bmatrix} 1, 5, 2, 3, 4 \\ 1, 2, 3, 4, 5 \end{bmatrix}$$

$$g = \begin{bmatrix} 1, 5, 2, 4, 3 \\ 1, 2, 3, 4, 5 \end{bmatrix}$$

$$h = \begin{bmatrix} 2, 1, 3, 4, 5 \\ 1, 2, 3, 4, 5 \end{bmatrix}$$

La sustitución f es *impar* porque su permutación imagen presenta tres inversiones: (5, 2); (5,3); (5,4).

La sustitución g es *par* porque su permutación imagen tiene cuatro inversiones: (5, 2); (5, 4); (5, 3); (4, 3).

La sustitución h es *impar* porque su permutación imagen posee una inversión: (2, 1).

Es frecuente decir que la *signatura* de una sustitución par es $+1$, asignándole el valor -1, si se trata de una sustitución impar.

Así, en el ejemplo anterior, las signaturas son:

$$s(f) = -1 \quad ; \quad s(g) = +1 \quad ; \quad s(h) = -1$$

Prescindiendo de su demostración, enunciaremos, sin embargo, el siguiente

TEOREMA. El producto de dos sustituciones de igual signatura produce una sustitución de signatura $+1$; si son de distinta signatura, su producto tiene de signatura -1.

Establecido el teorema precedente, destacaremos los tres siguientes corolarios, de los que conviene que el lector constate su clara justificación, sobre los ejemplos que se vienen estableciendo:

COROLARIO 1. La signatura del producto de dos transposiciones es siempre $+1$.

COROLARIO 2. Toda sustitución de signatura $+1$ se puede descomponer en un número par de transposiciones.

COROLARIO 3. Toda sustitución de signatura -1 se puede descomponer en un número impar de transposiciones.

2.45. GRUPOS MONOGENOS: GRUPOS CICLICOS; GENERADORES

Se define que el grupo $[G, *]$ es *monógeno* si está formado por los compuestos de un único elemento x, que se denomina *generador*.

En notación potencial, un grupo monógeno toma la forma

$$G = \{\ldots x^{-k}, \ldots x^{-2}, x^{-1}, x^0, x^1, x^2, \ldots x^k, \ldots\}$$

La notación potencial puede inducir a falsas interpretaciones cuando se trata de grupos monógenos aditivos; por ejemplo, $[Z, +]$ es un grupo monógeno aditivo cuyo generador pueden ser dos de sus elementos: el $(+1)$ y el (-1).

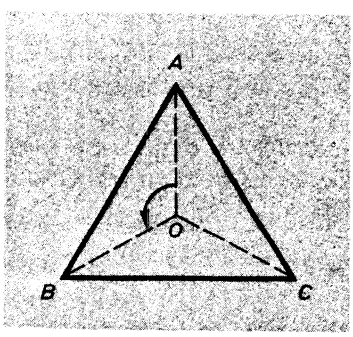
Tomamos el generador $(+1)$, y paralelamente escribimos, en tres líneas, la simbolización potencial, su significado operativo y finalmente, su símbolo entero:

$$Z=\{\ldots;\ (+1)^{-2}\ ;\ (+1)^{-1};\ (+1)^0;\ (+1)^1;\ (+1)^2\ ;\ (+1)^3\ ;\ldots\}$$
$$Z=\{\ldots;\ op(+1)+op(+1);\ op(+1);\ (0)\ ;\ (+1)\ ;\ (+1)+(+1);\ (+1)+(+1)+(+1);\ldots\}$$
$$Z=\{\ldots;\ (-2)\ ;\ (-1)\ ;\ (0)\ ;\ (+1)\ ;\ (+2)\ ;\ (+3)\ ;\ldots\}$$

Se llama *grupo cíclico* a un grupo monógeno finito

Ejemplo

Sobre el triángulo equilátero de la figura consideramos el subgrupo de isometrías



$$G = \{G_{0°}, G_{120°}, G_{-120°}, G_{240°}\}$$

El grupo de giros G del triángulo equilátero sobre su centro 0 es un grupo cíclico de tercer orden, cuyo generador es el elemento $G_{120°}$. En efecto:

$$(G_{120^\circ})^{-1} = G_{-120^\circ}; \quad (G_{120^\circ})^0 = G_{0^\circ}; \quad (G_{120^\circ})^1 = G_{120^\circ};$$
$$(G_{120^\circ})^2 = G_{120^\circ} \times G_{120^\circ} = G_{240^\circ}$$
$$G = \{(G_{120^\circ})^0; \quad (G_{120^\circ})^1; \quad (G_{120^\circ})^2\}$$

2.46. SUBGRUPOS

2.461. Establecimiento

Establecido un grupo $[G, *]$, se dirá de un $H \subset G$, $(H \neq \phi)$ que es un subgrupo del grupo establecido, si $[H, *]$ también tiene estructura de grupo.

Adviértase que todo grupo tiene dos subgrupos impropios: él mismo y el subconjunto unitario cuyo único elemento es el neutro de $[G, *]$.

Aparte de estos dos subgrupos citados, para que $[H, *]$ sea subgrupo de $[G, *]$, es claro que H ha de ser estable para $*$ (revísese 2.33 del capítulo anterior); que ha de contener el elemento neutro del grupo $[G, *]$; y que $\forall x \in H$, su simétrico x' también ha de pertenecer a H.

Todas estas condiciones pueden condensarse en el siguiente

2.462. Teorema

La condición necesaria y suficiente para que un $H \subset G$ sea subgrupo de G es que $\forall a \in H$ y $\forall b \in H$, si $a * b' = c \Rightarrow c \in H$.

Simbólicamente:

$$H \subset G \text{ es subgrupo de } G \Leftrightarrow \forall a \in H, \forall b \in H, a * b' = c \Rightarrow c \in H$$

Demostración

D_1) Condición necesaria: Hipótesis. H es subgrupo de G
Tesis. $(a * b') \in H$
Demostración. $b \in H \Rightarrow b' \in H$
$a \in H$ (por hipótesis)
$a * b' \in H$ (subconjunto estable)

D_2) Condición suficiente: Hipótesis. $a * b' \in H$
Tesis. H es subgrupo de G
Demostración. Uniformidad (por hipótesis)
Asociatividad (ya que $H \subset G$)
Elemento neutro:

$\varepsilon \in H$ (ya que $a * a' = \varepsilon$)
$\varepsilon * b' = b'$

Elementos simétricos:

$\varepsilon \in H$
$\varepsilon * b' \in H$ (por hipótesis)
$\Downarrow$
$b' \in H, \forall b \in H$

$[H, *]$, pues, tiene estructura de grupo: H es subgrupo de G.

Ejemplo

En el grupo de las isometrías directas planas $[M, \times]$, el conjunto de las traslaciones T es un subgrupo de M, ya que:

$T_j \times T_i = T_k$ (T es estable para el producto de isometrías).
$T_k \times (T_j \times T_i) = (T_k \times T_j) \times T_i$ (asociatividad de la adición de «vectores-guía»).
$I \times T_i = T_i \times I = T_i$ (I es elemento neutro: vector $\{\vec{0}\}$).
$T_i^- \times T_i \times T_i^- = I$ (elementos simetrizables: adición de vectores opuestos).

2.47. EL GRUPO DE LAS TRANSFORMACIONES

2.471. Ley de composición externa: operadores

En la definición de ley de composición interna se establecía una aplicación del cartesiano $A \times A$ en el propio A, de modo que un conjunto «generaba» todo el proceso.

Piénsese en un cartesiano de dos conjuntos distintos, aplicado sobre un tercer conjunto, que también puede ser distinto

$$A \times B \xrightarrow{\Phi} C$$

Tal aplicación Φ es una ley de composición externa

Ejemplo

La potenciación de naturales con exponentes enteros produce racionales

$$2^{-3} = \frac{1}{8}$$

$$\Phi(2, -3) = \frac{1}{8}; \; 2\,\Phi(-3) = 1/8$$

$$N \times Z \xrightarrow{\Phi} Q$$

Definición.

$$A \times B \xrightarrow{\Phi} C \text{ es ley de c. ext.} \Leftrightarrow \forall a \in A,\ \forall b \in B,\ \exists^* c \in C/\ \Phi(a, b) = c$$

o más usualmente,

$$/a \Phi\, b = c$$

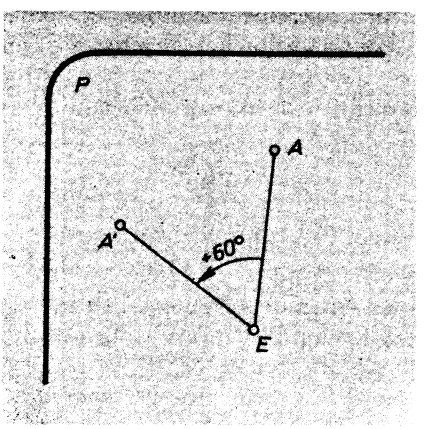
Resulta especialmente interesante el caso en que el conjunto de imágenes coincide con el conjunto multiplicando; es decir:

$$A \times B \xrightarrow{\Phi} A$$

Ejemplo

Entendemos por P el conjunto de puntos del plano y por G_E el conjunto de giros, de centro el punto E.

A cada punto $p \in P$, cada $G_i \in G_E$ le hace corresponder un $G_i(p) \in P$. Así, pues, queda establecida de este modo una ley de composición externa.



$$P \times G_E \xrightarrow{\Phi} P$$

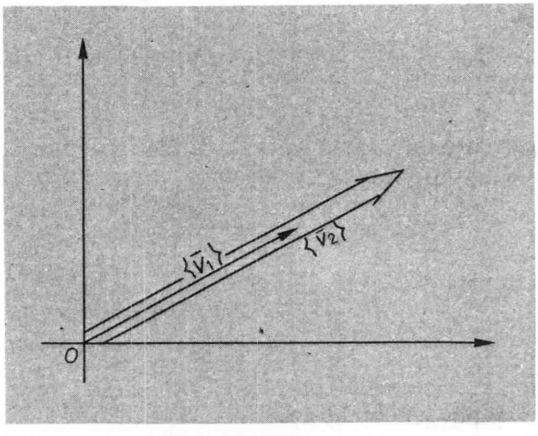
$$(A, G_{60°}) \xrightarrow{\Phi} \Phi(A, G_{60°}) = A'$$

$$A \Phi\, G_{60°} = A'$$

Otro *ejemplo* extraordinariamente importante, porque —en su momento— nos permitirá crear la estructura de espacio vectorial, es la ley de composición externa

$$V_2 \times R \xrightarrow{\Phi} V_2$$

en la que se simboliza: V_2 = conjunto de vectores libres del plano;
R = conjunto de los números reales.



$$\{\bar{v}_1\} \times 3/2 = \{\bar{v}_2\}$$

Puede sensibilizarse, en sugerente metáfora, el «oficio» que desempeñan los elementos del conjunto multiplicador del cartesiano original, en una ley de composición externa:

En la ley de composición externa, simbolizada

$$A \times B \xrightarrow{\Phi} C,$$

los elementos de A son como los materiales a elaborar, que entraran en fábrica; los elementos de B son los instrumentos, el «utillaje», que actuando sobre la «materia prima» A, produce los «manufacturados», que representarían a los elementos de C; entonces, Φ sería la «pauta de fabricación», que indica cómo han de usarse el conjunto de herramientas (elementos de B).

Operador es cada uno de los elementos del conjunto multiplicador del cartesiano original, en una ley de composición externa.

2.472. Operadores con estructura de grupo

Existen suficientes situaciones reales que, al matematizarlas, hacen surgir leyes de composición externa cuyo conjunto de operadores está estructurado —mediante una ley de composición interna— en forma de grupo.

(A partir de ahora —y si nada se especifica en contrario— estableceremos leyes de composición externa con el conjunto de imágenes igual al conjunto multiplicando del cartesiano original.)

$$A \times B \xrightarrow{\Phi} A$$

Se dice que B es un *grupo de operadores* sobre A, si existe una ley de composición interna en B, $*$, de modo que $[B, *]$ es un grupo.

Además, en este caso, se cumplen estas dos propiedades

I. $a\Phi\,(f * g) = (a\Phi\, f)\Phi\, g$ (léase nota contigua).

II. Si I es el neutro del grupo de operadores $[B, *]$,

$$\forall a \in A, \quad I\Phi\, a = a$$

NOTA. Esperamos que la notación usada —nada frecuente— sirva, sin embargo, para resaltar la naturaleza de *operaciones* de las aplicaciones que componen:

Operandos son las aplicaciones que denotamos con letras latinas (f, g, ...); signo operativo de la aplicación que compone, lo escribimos Φ.

Ello es análogo a usar el signo + así: $3 + 4 = 7$.

De todos modos, si al lector no le es necesaria tal distinción, transcribimos del modo usual aquí la propiedad I.

$$(g \cdot f)\,(a) = g[f(a)]$$

Este modo de escribir es análogo al uso del signo + de esta manera: $+\,(3, 4) = 7$.

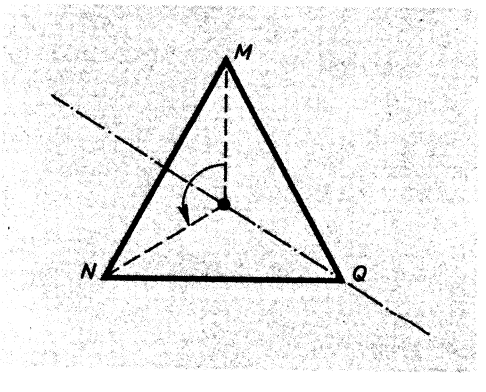
2.473. El grupo de las transformaciones

Un grupo de operadores B, que actuando sobre A cumple las dos últimas propiedades expuestas, se denomina «Grupo de transformaciones de A con el grupo operador B».

Ejemplo

«El grupo del triángulo equilátero»

1) Establezcamos sin más abstracción —lícita intuición positiva— el subconjunto de los puntos del plano $A = \{M, N, Q\}$, vértices del triángulo plano que se dibuja.



2) Establezcamos ahora el conjunto de transformaciones B, sobre A, de las siguientes simetrías y giros:

$$B = \{s_M, s_N, s_Q, g_{0°}, g_{120°}, g_{-120°}\}$$

2.1) Que B sea el conjunto de transformaciones anteriormente dicho, exige que se establezca una ley de composición interna en B, llamada «producto de movimientos»; y que esa ley dote a B de estructura de grupo, es decir, $[B, \times]$ tiene estructura de grupo.
(Entendemos que para el lector es harto conocido el producto de transformaciones geométricas y que está familiarizado con la «geometría concreta de la regla y compás». Si no es así, construya sobre seguro: consulte nuestros libros «Hacia la Matemática» o cualquiera otros de similar intencionalidad iniciadora).

2.2) Destaquemos también la verificación de las dos propiedades establecidas, últimas en la descripción de Grupo de transformaciones.

3) Así, pues, disponemos de:
   a) un conjunto de puntos $A = \{M, N, Q\}$
   b) un conjunto de operadores $B = \{s_M, s_N, s_Q, g_{0°}, g_{120°}, g_{-120°}\}$
   c) una ley de composición externa

$$A \times B \xrightarrow{\Phi} A,$$

siendo B grupo de operadores sobre A: $[B, \times]$.

Construyamos ahora la tabla de la ley interna del grupo de operadores, conviniendo en leer los operandos, el primero en la fila y el segundo en la columna donde aparezcan:

$\times$	s_M	s_N	s_Q	$g_{0°}$	$g_{120°}$	$g_{-120°}$
s_M	I	$g_{-120°}$	g_{120}	s_M	s_Q	s_N
s_N	$g_{120°}$	I	$g_{-120°}$	s_N	s_M	s_Q
s_Q	$g_{-120°}$	$g_{120°}$	I	s_Q	s_N	s_M
$g_{0°}$	s_M	s_N	s_Q	I	$g_{120°}$	$g_{-120°}$
$g_{120°}$	s_N	s_Q	s_M	$g_{120°}$	$g_{-120°}$	I
$g_{-120°}$	s_Q	s_M	s_N	$g_{-120°}$	I	$g_{120°}$

Dispuesta la tabla (obsérvese, de paso, que el grupo de operadores no es conmutativo, pues la tabla no es simétrica respecto a su diagonal principal), podemos comprobar, en algún caso, las dos propiedades que completan la definición de «grupo de transformaciones»; veamos:

I. *a*) Compongamos, según $\times$, dentro del grupo de operadores B:

b) comprobemos que en la ley de composición externa Φ,

$$Q \,\Phi\, g_{120°} = N, \text{ y que}$$
$$N \Phi\, s_M = Q$$

c) Veamos el compuesto de Q con la transformación producto s_Q:

$$Q \,\Phi\, s_Q = Q,$$

es decir (en notación convencional):

$$(s_M \times g_{120°})\,(Q) = s_M[g_{120°}\,(Q)] = Q$$

II. $I(Q) = Q$

2.474. Orbita de *a* generada por un grupo de operadores

Establezcamos un conjunto A y sobre él, un grupo de transformaciones B, que actúa según la ley externa

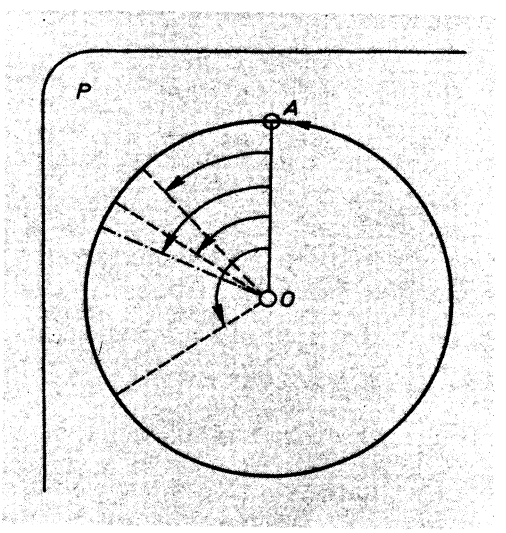
$$A \times B \xrightarrow{\Phi} A$$

Para cada elemento a del multiplicando A, se denomina *órbita de a* al subconjunto del conjunto de imágenes A, formado por todos los resultados de aplicar cada operador de B al elemento a considerado. O sea:

$$\left.\begin{array}{l} \forall a \in A, \text{ órbita de } a \\ \text{es } a_B \subset A \end{array}\right\} \Leftrightarrow a_B = \{x \,/\, \forall f \in B,\ x = f(a)\}$$

Ejemplo

Muy de acuerdo con el significado intuitivo de la palabra «órbita», establecemos el siguiente ejemplo:



P = conjunto de los puntos del plano;
$[G, \times]$ = grupo de todos los giros de centro O, operadores sobre P;

$P \times G \xrightarrow{\Phi} P$: ley de composición externa.

Como conjunto de puntos resultantes de la transformación, el plano P puede «intuirse» como el conjunto de circunferencias concéntricas de centro O y radios OA, para todo A del plano P.

Resulta claro, tal como se ha establecido el concepto de «órbita de un elemento a», que el conjunto-resultado de la ley externa, está formado por la reunión de subconjuntos disjuntos, cada uno de los cuales es la órbita de cada elemento original operado. Simbólicamente:

$$A = \{a, b, c\}$$
$$B = \{f, g, h, \ldots\}$$
$$A \times B \xrightarrow{\Phi} A$$
$$A = \{a_B\} \cup \{b_B\} \cup \{c_B\}$$

Adviértase que hemos llegado a una partición en el conjunto final A, a partir del concepto de órbita, lo que implica que existe una relación de equivalencia, agente de la clasificación correspondiente. El criterio de esa relación $\mathfrak{R}$ sería:

$$\forall a_1 \in A, \forall a_2 \in A, \quad a_1 \mathfrak{R} a_2 \Leftrightarrow a_2 \in a_{1_B},$$

dejando a la oportunidad, conveniencia o interés del lector, probar que —en efecto— la relación $\mathfrak{R}$ establecida es de equivalencia y, por tanto, agente de clasificación.

2.48. CONJUNTO COCIENTE, MODULO UN SUBGRUPO

2.481. Clases adjuntas

Sea el grupo $[G, \times]$ y un subgrupo de él, $[H, \times]$.
Se establece la ley de composición «externa»

$$G \times H \xrightarrow{\Phi} G$$
$$(a, f) \longrightarrow f(a),$$

en la que el conjunto-multiplicador del cartesiano es el subgrupo considerado, H.

Si se justifican las dos propiedades del párrafo 2.472, quedará establecido H como un *grupo de operadores*, que actuando sobre G, constituye un grupo de transformaciones de G.

En efecto: sean $a \in G$, $f \in H$ y $g \in H$.

1) Teniendo en cuenta que la ley interna es común a G y a H,

$$(g \times f)(a) = (g \times f) \times a;$$

2) como la ley $\times$ es asociativa,

$$(g \times f) \times a = g \times (f \times a);$$

3) por la misma razón que en 1),

$$g \times (f \times a) = g[f(a)].$$

Es decir:

$$\boxed{\text{I.} \quad (g \times f)(a) = g[f(a)]}$$

Siendo I el neutro del grupo $[H, \times]$,

$$I(a) = I \times a = a;$$

o sea:

$$\boxed{\text{II.} \quad I(a) = a}$$

Así, pues, queda establecido el subgrupo H, como grupo de operadores sobre G. Tratemos ahora de establecer la órbita de un $a \in G$. Es ésta:

$$a_H \equiv \{x/\forall f \in H, x = f(a)\}$$

Explicitando el carácter operativo de $f(a)$, y denotando la órbita del modo convencional que para este caso se usa, se escribe:

$$H \times a \equiv \{x/\forall f \in H, x = f \times a\}$$

También, en el caso concreto que se describe, las órbitas tienen nombre propio: se llaman *clases adjuntas*, y por su modo de construirlas, *clases adjuntas por la derecha**. No es poco frecuente encontrar otro nombre para estas órbitas, el de *clases residuales*. Tal denominación es una generalización de un caso particular tratado en la Aritmética clásica; ello será motivo de inmediato ejemplo.

Recuérdese que en el conjunto-resultado de la ley externa establecida aparece así una partición cuyos conjuntos disjuntos son cada una de las clases adjuntas; y que tal partición implica la clasificación del conjunto de resultados, G, quedando establecido el conjunto cociente G/H, cuyos elementos son las órbitas o clases adjuntas

$$G/H = \left\{\{H \times a\}, \{H \times b\}, \ldots\right\}$$

---

* Analógicamente se desarrolla toda la teoría para clases adjuntas por la izquierda. Bastará para ello establecer la aplicación inicial, de modo que la clase adjunta de a sea

$$a \times H = \{x/\forall f \in H, \; x = a \times f\}$$

Ejemplo

Sea el grupo aditivo $\{Z, +\}$ y considérese el $H \subset Z$,

$$H = \{x/(x \in Z) \wedge (x = \dot{5})\}$$

Es decir, H está formado por todos los múltiplos de 5.
— Usando el teorema correspondiente, se justifica que H es un subgrupo de Z.
— Tomando como módulo H, se establecen las clases adjuntas, que serán:

1.ª) el propio $\{H\}$, cuyos elementos son todas las imágenes que resultan al aplicar la adición a todos los múltiplos de 5, pertenecientes a Z.

$$(25 \in Z, \dot{5} \in H, 25 + \dot{5} = \dot{5} \in H);$$

es decir, todos los enteros que al dividirlos por 5, dan de resto 0;

2.ª) una $\{H + 1\}$, formada por todos los enteros que sumados con un múltiplo de cinco, producen un $\dot{5} + 1$

$$(16 \in Z, \dot{5} \in H, 16 + \dot{5} = \dot{5} + 1 \in H + 1);$$

es decir, todos los enteros que al dividirlos por 5, dan de resto 1;

3.ª) una $\{H + 2\}$, formada por todos los enteros que sumados con un múltiplo de cinco producen un $\dot{5} + 2$

$$(27 \in Z, \dot{5} \in H, 27 + \dot{5} = \dot{5} + 2 \in H + 2);$$

es decir, todos los enteros que al dividirlos por 5 dan de resto 2;

4.ª y 5.ª) unas $\{H + 3\}$ y $\{H + 4\}$, generadas análogamente a las anteriores.

De modo que el conjunto cociente de clases adjuntas, mejor en este caso, clases residuales módulo 5 es

$$Z/H = \left\{\{H\}, \{H + 1\}, \{H + 2\}, \{H + 3\}, \{H + 4\}\right\}$$

Retornando a la escritura convencional aritmética, se toma como representante canónico de cada clase, precisamente el propio resto, y el genérico H se denota por 5, quedando así el conjunto de las clases residuales, módulo 5

$$Z/5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

No siempre resulta fácil tabular el conjunto cociente G/H, con lo que todas las clases adjuntas quedan explicitadas. Conviene tener un criterio que permita discernir si dos elementos del grupo G pertenecen o no a la misma clase adjunta. Tal criterio está construido y es el siguiente

2.482. Teorema

La condición necesaria y suficiente para que dos elementos r y s de un grupo $[G, \times]$ pertenezcan a la misma clase adjunta (por la derecha), respecto del subgrupo H, es que $r \times s^{-1} \in H$. O sea:

$$\left.\begin{array}{l} r \in G;\ s \in G \\ \text{Si } \{H \times a\} \in G/H, \\ r \in \{H \times a\},\ s \in \{H \times a \end{array}\right\} \Leftrightarrow r \times s^{-1} \in H$$

Demostración:

D_1) Condición necesaria

H. $r \in \{H \times a\};\quad s \in \{H \times a\}$

T. $r \times s^{-1} \in H$

D. $r = f \times a;\quad s = g \times a \quad (f \in H, g \in H)$

$$r \times s^{-1} = (f \times a) \times (g \times a)^{-1} =$$

$\Downarrow$ Ya que G es grupo

$$= (f \times a) \times (a^{-1} \times g^{-1}) =$$

$\Downarrow$ Por asociatividad

$$= f \times (a \times a^{-1}) \times g^{-1} =$$

$\Downarrow$ Por la naturaleza de elementos simétricos, denotando el neutro por I

$$= f \times I \times g^{-1} =$$

$$= f \times g^{-1},$$ que obviamente, pertenece a H; $f \times g^{-1} \in H$.

D_2) Condición suficiente

H. $r \times s^{-1} \in H$

T. $r \in \{H \times a\};\ s \in \{H \times a\}$

D. *A*) $s = I \times s \in \{H \times s\}$ [1]

B) Sea un $t \in H$ el resultado que se expresa:

$$r \times s^{-1} = t$$

Componiendo por la derecha con s:

$$(r \times s^{-1}) \times s = t \times s$$

Asociatividad:

$$r \times (s^{-1} \times s) = t \times s$$

Elementos simétricos

$$r \times I = t \times s$$

Elemento neutro

$$r = t \times s;$$

o lo que es lo mismo:

$$r = s(t).$$

O sea:

$$r \in \{H \times s\} \qquad [2]$$

Con [1] y [2] queda demostrada la tesis, asignando al genérico a el específico s.

2.483. Indice de *H* en *G*. Teorema de Lagrange

Se denomina *índice de H en G* al cardinal del conjunto cociente $\{G/H\}$.

TEOREMA. El índice de H en G es divisor del orden del grupo finito G; o con más rigor «histórico»: el orden de H divide al orden de G. Es decir:

$$\text{card}(G) = \text{card}(G/H) \times \text{card}(H)$$

En efecto: sea un G de orden n y sea también un $a \in G$. Además

$$H = \{f_1, f_2, \ldots, f_i, \ldots f_k, \ldots, f_m\}$$

Resulta obvio que $m \leq n$.
La clase adjunta de a será:

$$H \times a = \{f_1(a), f_2(a), \ldots f_i(a), \ldots f_k(a), \ldots f_m(a)\},$$

o lo que es igual:

$$H \times a = \{f_1 \times a, f_2 \times a, \ldots f_i \times a, \ldots f_k \times a, \ldots f_m \times a\}.$$

A) Siendo el orden de H, m, cada una de las clases adjuntas $H \times a \in \{G/H\}$ tienen también m elementos*.
B) Todas las clases adjuntas son disjuntas.
C) Todo a perteneciente a G, pertenece a una única clase $H \times a$.
Las tres afirmaciones precedentes concluyen la tesis.

---

* Basta demostrar que si $f_i \neq f_k \Leftrightarrow f_i \times a \neq f_k \times a$.
Demostración al absurdo: Veamos que si la tesis es la contraria, la hipótesis no se mantiene:

$$f_i \times a = f_i \times a \Rightarrow (f_i \times a) \times a^{-1} = (f_k \times a) \times a^{-1} \Leftrightarrow f_i \times (a \times a^{-1}) = f_k \times (a \times a^{-1})$$
$$\Updownarrow$$
$$f_i = f_k$$

2.484. Subgrupos normales, invariantes o distinguidos

Sea un grupo finito $[G, \times]$ y un subgrupo de él, H.

Se dirá de H que es un subgrupo normal de G, si las clases adjuntas por la derecha y por la izquierda coinciden. Es decir:

$$\forall a \in G \quad , \quad a \times H = H \times a$$

Resulta fácil demostrar que si $[G, \times]$ es abeliano, cualquier subgrupo suyo es normal.

2.485. Grupo cociente del grupo *G* respecto del subgrupo invariante *H*

La gran importancia de los subgrupos normales o invariantes radica en que el conjunto cociente de clases adjuntas que generan $\{G/H\}$ puede estructurarse, a su vez, en forma de grupo, mediante una ley inducida por la ley del grupo G.

1) Establecimiento de la ley inducida

Sean las dos clases adjuntas biláteras*

$$\{a \times H\} \in \{G/H\}$$
$$\{b \times H\} \in \{G/H\}$$

La operación inducida en $\{G/H\}$ se establece así:

$$\{a \times H\} \bar{\times} \{b \times H\} = \{(a \times b) \times H\}$$

2) Análisis de la ley inducida

2*a*) Es ley de composición interna, ya que, como $(a \times b) \in H$, el resultado siempre pertenece a $\{G/H\}$

2*b*) Es asociativa

$$(a \times H) \bar{\times} [(b \times H) \bar{\times} (c \times H)] = (a \times H) \bar{\times} [(b \times c) \times H] =$$
$$= [a \times (b \times c)] \times H = [(a \times b) \times c] \times H = [(a \times b) \times H] \bar{\times}$$
$$\bar{\times} (c \times H) = [(a \times H) \bar{\times} (b \times H)] \bar{\times} (c \times H)$$

2*c*) Tiene clase neutra

Siendo ε el elemento neutro de G, la clase $\{\varepsilon \times H\}$ es precisamente la clase neutra del grupo $[G/H, \bar{\times}]$. En efecto:

Sea una clase $\{a \times H\} \in \{G/H\}$:

$$\{a \times H\} \bar{\times} \{\varepsilon \times H\} = \{(a \times \varepsilon) \times H\} = \{a \times H\};$$

---

* Indistintamente, adjuntas por la derecha o por la izquierda.

y también,

$$\{\varepsilon \times H\} \bar{\times} \{a \times H\} = \{(\varepsilon \times a) \times H\} = \{a \times H\}$$

2*d*) Todas las clases son simetrizables. En efecto:

$$\forall \{a \times H\} \in \{G/H\}, \quad \exists^* \{a^{-1} \times H\} \in \{G/H\} / \{a \times H\} \bar{\times} \{a^{-1} \times H\} = \{(a \times a^{-1}) \times H\} = \{\varepsilon \times H\}$$

3) Conclusión

El conjunto cociente respecto del subgrupo normal H, $\{G/H\}$, ha sido estructurado —a su vez— como grupo con la ley inducida $\bar{\times}$.

$[\{G/H\}, \bar{\times}]$ es el grupo cociente respecto del subgrupo normal H.

2.49. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

2.490.

El conjunto de las raíces en $\mathbb{C}$ de la ecuación $x^4 - 1 = 0$ es un grupo multiplicativo abeliano de orden 4.

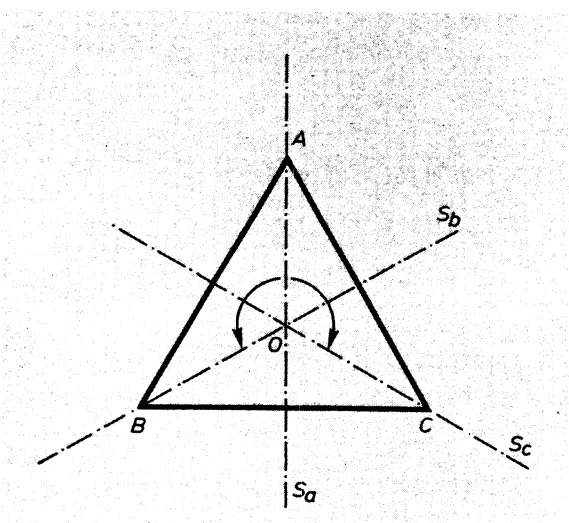
Establézcase la tabla del grupo y compruébese que —en efecto— posee la estructura que se indica.

2.491.

Determínense todos los subgrupos propios del grupo del ejercicio anterior.

2.492.

Sobre el triángulo de la figura se establecen las isometrías que se indican y que ya fueron descritas en el ejemplo del número 2.42:



a) Inténtese realizar la tabla del grupo. Luego, compruébese si es correcta, comparándola con la del ejemplo del número 2.473.

b) Determínense todos los subgrupos propios de este grupo de movimientos.

2.493.

Demuéstrese que si $[G, \times]$ es un grupo abeliano, cualquier subgrupo suyo es normal.

2.494.

Sobre el conjunto $A = \{\alpha, \beta, \gamma\}$ se define la operación $*$, de modo que $[A, *]$ alcanza estructura de grupo abeliano.

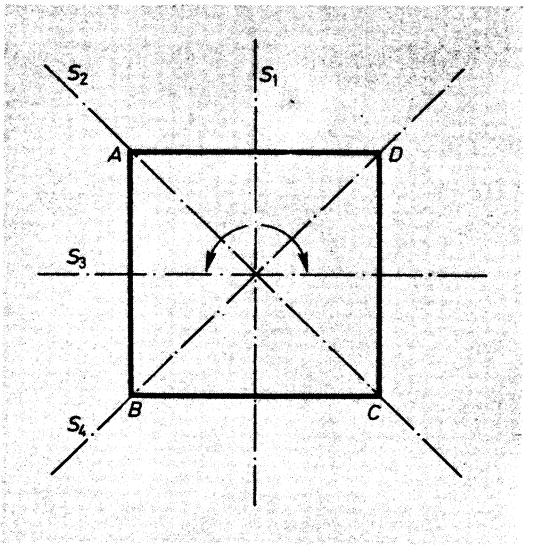
Establézcase la tabla del grupo.

2.495.

Sobre el cuadrado de la figura se consideran las isometrías

g_0 = giro de centro 0 y amplitud 0°
g_1 = giro de centro 0 y amplitud 90°
g_2 = giro de centro 0 y amplitud −90°
g_3 = giro de centro 0 y amplitud 180°

s_1 = simetría axial de eje s_1
s_2 = simetría axial de eje s_2
s_3 = simetría axial de eje s_3
s_4 = simetría axial de eje s_4



Como es sabido, el conjunto $G = \{g_0, g_1, g_2, g_3, s_1, s_2, s_3, s_4\}$ tiene estructura de grupo respecto del producto de transformaciones. Sea S el conjunto de las simetrías planteadas. Se pregunta:

a) ¿Es $[S, \times]$ un subgrupo de G? Justifíquese su respuesta;

b) ¿Lo es el conjunto H de los giros establecidos? Justifíquese que —en efecto— H es un subgrupo de G.

c) Constrúyanse las clases adjuntas por la derecha módulo el subgrupo H.

d) ¿Es indiferente haberlas construido por la izquierda? Justifíquese su contestación, que ha de ser afirmativa.

e) ¿Es H un subgrupo invariante de G?

f) ¿Es posible que le «hayan salido» tres clases adjuntas? ¿Qué criterio prohíbe, *a priori*, tal número?

g) ¿Se puede estructurar el conjunto de clases G/H como grupo? Razónese.

2.496.

En $Q \times Q$ se establece la ley $(a, b) * (c, d) = (ac, bc + d)$. Muéstrese que la operación establecida en $Q \times Q$ estructura a ese cartesiano en forma de grupo no abeliano.

2.497.

Continuando con el ejercicio anterior, demuéstrese que $H \subset (Q \times Q)$

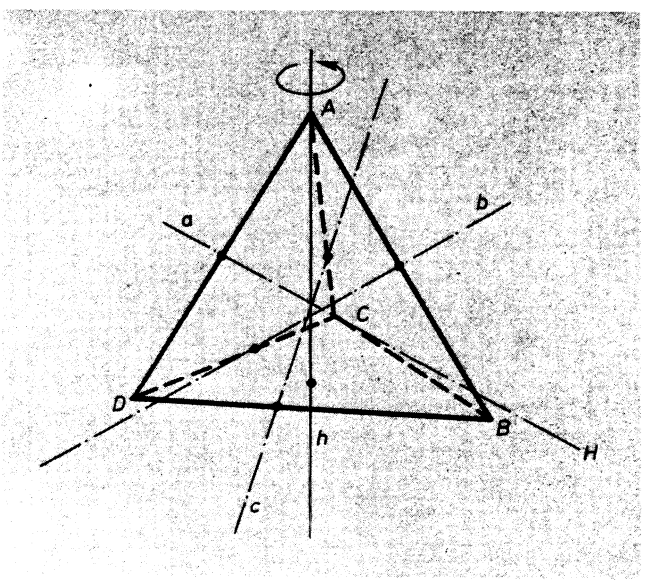
$$H = \{(1, \times)/x \in Q\},$$

es un subgrupo de $Q \times Q$.

2.498.

Sea el tetraedro regular de la figura y considérense el conjunto de transformaciones

g_0 = giro de eje h y amplitud 0º
s_1 = simetría de eje a
s_2 = simetría de eje b
s_3 = simetría de eje c



Establecido el conjunto de operadores $H = \{g_0, s_1, s_2, s_3\}$ sobre el conjunto de los vértices del tetraedro $P = \{A, B, C, D\}$, se obtienen, entre otras, estas dos sustituciones:

$$s_2 = \begin{pmatrix} B & A & D & C \\ A & B & C & D \end{pmatrix} \qquad s_3 = \begin{pmatrix} C & D & A & B \\ A & B & C & D \end{pmatrix}.$$

1) Escríbanse la g_0 y la g_1

2) Realícense todos los productos de operadores, como se realiza el que se escribe:

$$s_3 \times s_2 = \begin{pmatrix} D & C & B & A \\ A & B & C & D \end{pmatrix} = s_1$$

3) Constrúyase la tabla del grupo $[H, \times]$, comprobando que es abeliano.
4) Compruébense las dos propiedades que se han de cumplir, como grupo de transformaciones que es.

2.499.

Constrúyase el grupo aditivo de las funciones escalonadas

$$y = \left[\frac{x}{m}\right], \text{ en } [a, b].$$

2.49.10.

Desarróllense los dos ejemplos del número 2.42.

2.5

Homomorfismo

2.51. Establecimiento del concepto de homomorfismo

2.52. Imagen homomorfa de un grupo $[A, *]$

2.521. *Definición*
2.522. *Teorema*
2.523. *Teorema*
2.524. *Teorema*
2.525. *Teorema*

2.53. Homomorfismos canónicos o naturales

2.54. Nomenclatura

2.55. Equivalencia asociada a un homomorfismo

2.56. Núcleo de un homomorfismo

2.561. *Definición*
2.562. *Teorema*
2.563. *Teorema*

2.57. Isomorfismos de «inmersión»

2.58. Aplicabilidad. Automatismos y destrezas

2.5

Homomorfismo

2.51. ESTABLECIMIENTO DEL CONCEPTO DE HOMOMORFISMO

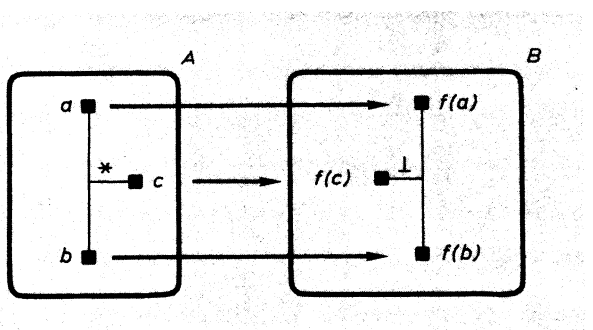
Considérense los grupos $[A, *]$ y $[B, \perp]$.

Establezcamos una aplicación f entre ambos grupos que satisfaga la siguiente propiedad:

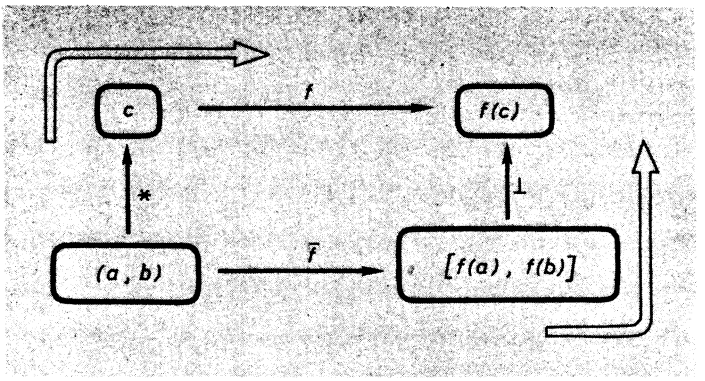
$$\forall a \in A, \quad \forall b \in A, \text{ si } a * b = c \Rightarrow f(a) \perp f(b) = f(c).$$

Toda aplicación como la establecida se llama homomorfismo.

«Visualicemos» este importante concepto, mediante un diagrama de Venn:



También es frecuente en la didáctica de este concepto utilizar este expresivo esquema:

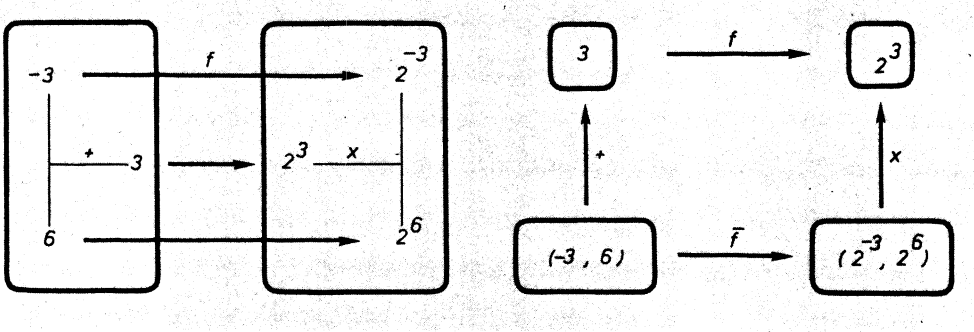


Con las flechas gruesas se quiere indicar que el homomorfismo produce el mismo resultado por los dos caminos señalados: si se opera el par $(a, b) \in A \times A$ con la operación $*$, se obtiene el resultado c, cuya imagen es $f(c)$; si, por el contrario, al par $(a, b) \in A \times A$ se le aplica primero el homorfismo «inducido» en el cartesiano, $\bar{f}$, se obtiene la imagen del par, $(f(a), f(b)) \in B \times B$ que, operado con la ley de su grupo, $\perp$, produce también $f(c)$.

Ejemplo

Sean los grupos $[Z, +]$ y $[Q - \{0\}, \times]$, y la aplicación $f: 2^{\times}$

$\forall x \in Z, \forall y \in Z,\ x + y = z \Rightarrow 2^x \cdot 2^y = 2^{x-y} = 2^z$



2.52. IMAGEN HOMOMORFA DE UN GRUPO $[A, *]$

2.521. Definición

Se denomina imagen homomorfa del grupo $[A, *]$ en $[B, \perp]$, mediante el homomorfismo f, al subconjunto de B, formado por todas las imágenes de los elementos del grupo $[A, *]$. Es decir, a un $B_1 \subset B$, tal que

$$f(A) \equiv B_1 \equiv \{f(x), x \in A\}$$

2.522. TEOREMA: La imagen homomorfa de cualquier subgrupo de $[A, *]$, mediante f, en $[B, \perp]$ es un subgrupo de B.

En efecto: sea A_1 un subgrupo de A, y x e y dos elementos de él; sean $p \in B$ y $q \in B$, tales que $p = f(x)$ y $q = f(y)$.

Si p y q pertenecen al mismo subgrupo B_1 de B, han de cumplir el teorema correspondiente (ver 2.462):

$$p \perp q' = f(x) \perp [f(y)]' = f(x) \perp f(y') = f(x * y')$$

Como $(x * y') \in A_1 \Rightarrow f(x * y') = (p \perp q') \in B_1$, c.q.d.

Corolario

La imagen homomorfa de $[A, *]$, mediante el homomorfismo f, en $[B, \perp]$ es un subgrupo de B.

Basta tener en cuenta que A es un subgrupo del propio $[A, *]$.

2.523. TEOREMA: La imagen recíproca de todo subgrupo de B es un subgrupo de A. Un razonamiento análogo al desarrollado en el teorema anterior, concluye la tesis. (Desarróllese como ejercicio.)

2.524. TEOREMA: La imagen del neutro de $[A, *]$ es el neutro de $[B, \perp]$.

Sean los neutros de ambos grupos $\varepsilon_1 \in A$ y $\varepsilon_2 \in B$.

Por la naturaleza de neutro de ε_1:

$$\forall x \in A, \quad x * \varepsilon_1 = \varepsilon_1 * x = x;$$

luego

$$f(x * \varepsilon_1) = f(x) \qquad [1]$$

Aplicando el homomorfismo f al par (x, ε_1),

$$f(x * \varepsilon_1) = f(x) \perp f(\varepsilon_1) \qquad [2]$$

Sustituyendo [1] en [2],

$$f(x) = f(x) \perp f(\varepsilon_1);$$

lo que indica que $f(\varepsilon_1)$ ha de ser el neutro de $[B, \perp]$.

Se concluye:

$$f(\varepsilon_1) = \varepsilon_2$$

2.525. TEOREMA: La imagen del simétrico de $x \in A$ es el simétrico de su imagen, $f(x) \in B$.

Sean $x \in A$ y $x' \in A \quad / \quad x * x' = x' * x = \varepsilon_1$

$$f(x * x') = f(\varepsilon_1) = \varepsilon_2 \Rightarrow f(x) \perp f(x') = \varepsilon_2$$
$$f(x' * x) = f(\varepsilon_1) = \varepsilon_2 \Rightarrow f(x') \perp f(x) = \varepsilon_2$$

Estos dos resultados definen como simétrico de $f(x)$ en $[B, \perp]$ el elemento $f(x')$. Es decir:

$$[f(x)]' = f(x')$$

2.53. HOMOMORFISMOS CANONICOS O NATURALES

Consúltese el número 2.485. Allí quedaba establecido el grupo cociente G/H, a que daba lugar un subgrupo normal H de G.

Se establece aquí una aplicación del grupo G en G/H, cuyo criterio es hacer corresponder a cada elemento de G, la clase de G/H a la que pertenece:

$$[G, \times] \xrightarrow{\varphi} [G/H, \bar{\times}]$$
$$a \longrightarrow \varphi(a) \equiv a \times H$$

Probemos que φ es homomorfismo:

$$\forall a \in G, \quad \forall b \in G, \quad \exists c \in G \,/\, a \times b = c$$

De otro lado,

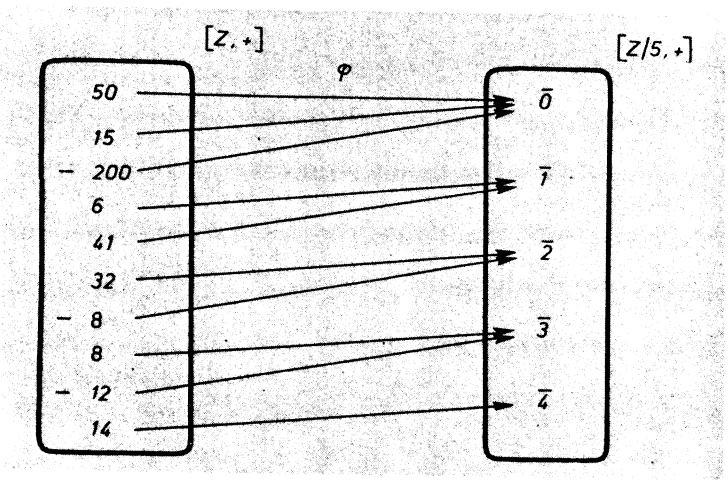
$$\varphi(a) \,\bar{\times}\, \varphi(b) = \{(a \times H)\} \,\bar{\times}\, \{(b \times H)\} = \{(a \times b) \times H\} = \{c \times H\} = \varphi(c).$$

Luego el compuesto de imágenes es igual a la imagen del compuesto, c.q.d.

Un homomorfismo como el descrito, establecido entre un grupo y uno de sus grupos cocientes, recibe el nombre de homomorfismo canónico o natural.

Continuando con el ejemplo del número 2.481, analicemos ahora que el conjunto cociente $Z/5$ se estructura en forma de grupo, ya que al ser $[Z, +]$ un grupo abeliano, cualquier subgrupo de él (en nuestro caso $H = \{\bar{5}\}$) es normal o invariante.

Así, pues, establezcamos la aplicación entre $[Z, +]$ y $[Z/5, +]$, que hace corresponder a cada $a \in Z$, su clase residual, módulo 5:



(Simbolizamos la ley inducida en $Z/5$ también con $+$)

Constatemos que se trata de un homomorfismo. Por ejemplo:

en $[Z, +]$: $6 + 8 = 14$

en $[Z/5, +]$: $\varphi(6) + \varphi(8) = \{\bar{1}\} + \{\bar{3}\} = \{\bar{4}\} = \varphi(14)$

De este modo ha quedado establecido un homomorfismo natural entre el grupo aditivo de los enteros y el grupo-cociente de las clases residuales, módulo 5.

2.54. NOMENCLATURA

Siendo los homomorfismos aplicaciones, aquellos podrán clasificarse análogamente a como se hace con éstas, con denominaciones específicas que se relacionan en el siguiente cuadro:

Homomorfismo: $[A, *] \xrightarrow{f} [B, \perp]$

Aplicación f	*Denominación*
No inyectiva, No exhaustiva	homomorfismo
Inyectiva	monomorfismo
Exhaustiva	epimorfismo
Biyectiva	isomorfismo

Endomorfismo = homomorfismo $A \to A$
Automorfismo = isomorfismo $A \to A$

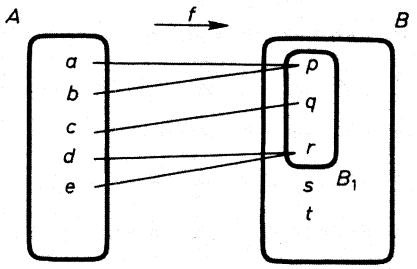
La destreza en manejar estas denominaciones ha de llegar a la fluidez necesaria para utilizar sustantivaciones o adjetivaciones complementarias, y que describen el mismo concepto; por ejemplo: un endomorfismo isomórfico es un automorfismo.

2.55. EQUIVALENCIA ASOCIADA A UN HOMOMORFISMO

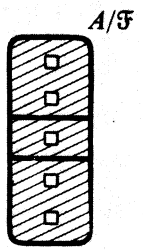
Sea el grupoide $[A, *]$ y B_1 su imagen homomorfa, mediante f, en $[B, \perp]$. La relación de equivalencia $\mathfrak{F}$, asociada a f, determina un conjunto cociente $A/\mathfrak{F}$, que es isomorfo con B_1, dotado de la ley $\perp$.

En efecto (simultanearemos los planteamientos matemáticos con apoyaturas didácticas gráficas).

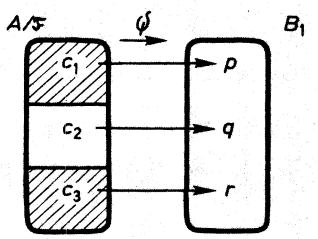
1)



2) Sea $\mathfrak{F}$ = «tener la misma imagen en B». Entonces el conjunto cociente $A/\mathfrak{F}$ es



3) Mediante una aplicación ψ entre $A/\mathfrak{F}$ y B_1, se hace corresponder biunívocamente, a cada clase, la imagen que la generó:



4) La ley $*$ de A induce en $A/\mathfrak{F}$ la ley $\bar{*}$ entre sus clases

$$a * c = e \Rightarrow \{c_1\} \bar{*} \{c_2\} = \{c_3\}$$

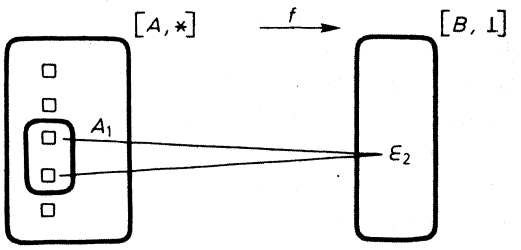
5) La biyección ψ es un isomorfismo entre los grupoides $[A/\mathfrak{F}, \bar{*}]$ y $[B_1, \perp]$:

$$\{c_1\} \bar{*} \{c_2\} = \{c_3\} \Rightarrow p \perp q = r$$

2.56. NUCLEO DE UN HOMOMORFISMO

2.561. Definición

Se establece el homomorfismo $[A, *] \xrightarrow{f} [B, \perp]$; sea ε_2 el neutro de $[B, \perp]$. Se llama núcleo de f al conjunto $A_1 \subset A / \forall x \in A_1,\ f(x) = \varepsilon_2$



En la bibliografía es usual denotar al núcleo de un homomorfismo f por la expresión «ker(f)»*.

2.562. TEOREMA: En el homomorfismo $[A, *] \xrightarrow{f} [B, \perp)$, ker($f$) es un subgrupo normal de A.

Demostración:

D_1) ker(f) es subgrupo de A.
Es obvio que si ker(f) sólo posee el neutro ε_1, el núcleo es subgrupo de A; si no es así, justifiquemos que para dos elementos a y b de ker(f) se cumple el teorema de existencia de subgrupo; recuérdese:

$$\text{si } a \in \ker(f),\ b \in \ker(f) \Rightarrow (a * b') \in \ker(f).$$

Veamos:

$$f(a) = \varepsilon_2 \quad ; \quad f(b) = \varepsilon_2$$

$$f(b') = [f(b)]' \quad \text{(Teorema 2.525.)}$$

Sustituyendo,

$$f(b') = [\varepsilon_2]' = \varepsilon_2$$

Con ello, calculemos:

$$f(a * b') = f(a) \perp f(b') = \varepsilon_2 \perp \varepsilon_2 = \varepsilon_2;$$

* Tal notación procede de que en alemán y en inglés «núcleo» se traduce por Kern y Kernel, respectivamente.

luego:

$$(a * b') \in \ker(f).$$

D_2) $\ker(f)$ es subgrupo normal de A.
Se demuestra que la condición necesaria y suficiente para que un subgrupo H lo sea normal de G, es que

$$\forall a \in G,\ \exists k \in H / (a * k * a') \in H$$

(Ver ejercicio 2.580.)

Usando, pues, de este teorema, veamos si la imagen de esa composición triple es ε_2:

$$\begin{aligned} f(a * k * a') &= f(a) \perp f(k) \perp f(a') = \\ &= f(a) \perp \varepsilon_2 \perp f(a') = \\ &= f(a) \perp [f(a)]' = \varepsilon_2, \text{ c.q.d.} \end{aligned}$$

2.563. TEOREMA: La condición necesaria y suficiente para que un homomorfismo sea monomorfismo (inyectivo) es que $\ker(f) \equiv \{\varepsilon_1\}$.

Demostración

1) Condición necesaria
Si f es inyectivo, $f(x) = \varepsilon_2 \Rightarrow f(x) = f(\varepsilon_1)$; $x \equiv \varepsilon_1$;
es decir:

$$\ker(f) \equiv \{\varepsilon_1\}.$$

2) Condición suficiente
Si $\ker(f) \equiv \{\varepsilon_1\}$, $f(x) = f(y) \Rightarrow f(x) \perp [f(y)]' = \varepsilon_2$
$f(x * y') = \varepsilon_2$;
o sea:

$$(x * y') \in \ker(f).$$

Como $\ker(f) = \{\varepsilon_1\}$, $(x * y') = \varepsilon_1$;
es decir: $x = y$;
luego f es una inyección.

2.57. ISOMORFISMOS DE «INMERSION»

Con ocasión de la simetrización de semigrupos para la creación de grupos, en el número 2.4323 se decía que el grupo creado «captaba» al semigrupo generador, que quedaba así «sumergido» en él.

Allí también quedó dicho que el sentido de esa «captación» se desarrollaría en este capítulo, cosa que pasamos a cumplir.

Nos parece indicado iniciar la cuestión, concretando sobre un ejemplo —bien conocido— para, finalmente, generalizar las conclusiones.

Ejemplo

1. Sea el semigrupo aditivo de los naturales, con el 0

$$[N \cup \{0\}, +]$$

que (recuérdese) es abeliano y cancelativo.

2. La ley adición del semigrupo establece para tres naturales

$$a + b = c$$

3. Sobre $N \times N$ se crea Z, mediante la relación de equivalencia R

$$(a, b)\, R\, (c, d) \Leftrightarrow a + d = b + c$$

$$Z = N \times N/R = \left\{ \{(a, b)\}, \{(e, f)\}, \ldots \right\}$$

4. Queda establecida entre las clases de Z la ley inducida «adición de enteros». Así:

$$\{(a, b)\} \tilde{+} \{(e, f)\} = \{(a + e, b + f)\}$$

5. Signando a partir de ahora la adición en Z con el habitual $+$, queda establecido el grupo aditivo de los enteros $[Z, +]$.
6. Considérese una aplicación f entre N y Z^+, cuyo criterio es el que se indica:

$$\begin{array}{l} N \xrightarrow{f} Z^+ \\ a \rightarrow f(a) = \{(a, 0)\} \end{array}$$

Esta f obviamente es un isomorfismo (compruébese).

7. De este modo, el vulgarismo «$N \subset Z$» queda justificado operativamente, ya que, aun cuando estructuralmente es «absolutamente falso», el isomorfismo entre N y Z^+ les confiere a ambos idéntica estructura y, por ende, idéntico comportamiento operativo; pero —se insiste— los elementos de N y los de Z^+ son «del todo distintos».
8. Terminemos con algunas consideraciones alrededor de un simple ejercicio. Una cuestión de escuela primaria es esta elemental, a primera vista, operación: Efectuar $5 + (-2)$.
   El niño avispado, que ha conseguido la «destreza de los signos», no duda en escribir

$$5 + (-2) = 5 - 2 = 3,$$

inconsciente del todo, de que ha manejado —¡nada menos!— dos veces el isomorfismo de inmersión que permite «homologar» los naturales a los enteros positivos.

Intentemos —por una vez— realizar el ejercicio con rigor estructural. Sería de este modo:

$$5 \in N \to f(5) = (5, 0) = (+5) \in Z$$

$$-2 \equiv (0, 2) \in Z$$

Adición en Z:

$$(5, 0) + (0, 2) = (5, 2) = (3, 0) = (+3)$$

$$(+3) \in Z \to f^{-1}(+3) = 3 \in N$$

Tras la inmediata generalización del concepto, insistiremos con otro ejemplo: el isomorfismo que permite «sumergir» Z en Q y que, de algún modo, legitima el vulgarismo «$Z \subset Q$».

Sea $[C, *]$ un semigrupo abeliano cancelativo.
Se establece la relación de equivalencia R en $C \times C$

$$(a, b)\, R\, (c, d) \Leftrightarrow a * d = b * c$$

Sea, finalmente, el conjunto cociente

$$C \times C/R = \left\{ \{(a, b)\}, \{(e, f)\}, \ldots \right\},$$

que en su lugar quedó estructurado en forma de grupo, mediante la ley inducida $\bar{*}$.

Considérense, $\forall a \in C$, los pares del cartesiano $C \times C$, del tipo $(a * x, x)$, $\forall x \in C$. Intentamos demostrar que todos los pares del tipo escrito pertenecen a la misma clase de $C \times C/R$. En efecto:

$$(a * x) * y = a * (x * y) = (a * y) * x = x * (a * y)$$

$$\Updownarrow$$

$$(a * x, x)\, R\, (a * y, y)$$

Recíprocamente, si

$$(a * x, x)\, R\, (p, q) \Rightarrow p = a * q.$$

En efecto:

$$(a * x, x)\, R\, (p, q) \Rightarrow (a * x) * q = x * p \Rightarrow a * x * q = x * p \Rightarrow a * q = p$$

Se establece ahora la aplicación f de C en $C \times C/R$, con el siguiente criterio:

$$C \xrightarrow{f} C \times C/R$$
$$a \to f(a) = \{(a * x, x)\},$$

de modo que a cada elemento de C le corresponde como imagen la clase de $C \times C/R$, anteriormente establecida.

Un inmediato análisis de f nos dice que es una inyección y también un homomorfismo; en fin, la f establecida es un monomorfismo.

Por último, si se restringe el monomorfismo f al subconjunto de $C \times C/R$, formado por las imágenes de C, aparece un monomorfismo epimórfico, es decir: un isomorfismo.

Tal isomorfismo es el que denominamos «isomorfismo de inmersión» que, de algún modo, permite «sumergir» el conjunto C en $C \times C/R$, como subconjunto suyo.

En realidad —se insiste— lo que se hace es «homologar» C a su conjunto-imagen isomórfico en $C \times C/R$.

Ejemplo

1. Sea el semigrupo multiplicativo abeliano cancelativo $[Z, \times]$.
2. Construyamos Q, mediante la relación de equivalencia R en $Z \times Z^0$,

$$(a, b)\, R\, (c, d) \Leftrightarrow a \times d = b \times c$$

$$Q = Z \times Z^0/R = \left\{ \left\{\frac{a}{b}\right\}, \left\{\frac{e}{f}\right\}, \ldots \right\}$$

3. Se establece entre las clases racionales de Q la ley multiplicación $\bar{\times}$, inducida por la multiplicación en Z. Así:

$$\left\{\frac{a}{b}\right\} \bar{\times} \left\{\frac{e}{f}\right\} = \left\{\frac{a \times e}{b \times f}\right\}$$

4. Signando, como es usual, la multiplicación en Q con el símbolo $\times$, queda establecido el grupo multiplicativo de los racionales, excepto el $\{0\}$.

$$[Q^0, \times]$$

5. Considérese ahora una aplicación f de Z en Q, cuyo criterio es el que se indica

$$Z \xrightarrow{f} Q$$

$$a \longrightarrow f(a) = \left\{\frac{a}{1}\right\}$$

Esta f, obviamente, es una inyección homomórfica, es decir, un monomorfismo.

6. Si se restringe f al conjunto imagen $\left\{\frac{Q}{1}\right\}$, se obtiene el isomorfismo de «inmersión» que «sumerge» Z en Q, y que, de algún modo, permite escribir $Z \subset Q$.

2.58. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

2.580.

La condición necesaria y suficiente para que un subgrupo H lo sea normal de G, es que $\forall a \in G,\ \exists k \in H / (a * k * a') \in H$.

Se justifica que es necesario, dejando al cuidado del lector completar la demostración.

Si H es normal, $a * k = j * a$ $(a \in G,\ j \in H,\ k \in H)$.

Componiendo por la derecha con el simétrico de a,

$$(a * k) * a' = (j * a) * a'$$

$$a * k * a' = j * (a * a') = j * \varepsilon = j \in H$$

2.581.

Justifíquese con rigor estructural esta operación elemental

$$3 + \frac{1}{5} = \frac{16}{5}$$

2.582.

Desarróllese ordenadamente la cuestión estructural que sugiere el siguiente esquema

$$\begin{array}{ccc} 6 & \xrightarrow{\log} & 0{,}778151 \\ \uparrow \times & & \uparrow + \\ (2,\ 3) & \xrightarrow{\log} & (0{,}301030;\ 0{,}477121) \end{array}$$

2.583.

Analícese, a la luz del homomorfismo $[Z, \times] \to [Z/9, \times]$, entre los enteros y el conjunto de clase residuales, módulo 9, la que en aritmética elemental se llamaba «prueba de los nueves» de la multiplicación. Resaltar su validez parcial.

2.584.

Sea A el conjunto de soluciones de la ecuación en Z, $x^3 - x = 0$. Se establece la aplicación $f: Z \longrightarrow A$, cuyo criterio es:

$$\begin{aligned} \forall x \in Z, f(x) = 0 &\Rightarrow x = 0 \\ f(x) = +1 &\Rightarrow x \in Z^+ \\ f(x) = -1 &\Rightarrow x \in Z^- \end{aligned}$$

Justifíquese que f es un homomorfismo entre $[Z, \times]$ y $[A, \times]$.

2.585.

Sea el semigrupo aditivo abeliano con elemento neutro de los naturales con el 0. Y considérese también el subconjunto $B = \{0, 1\}$, dotado de la adición.

Se establece una aplicación $f: N \to B$, de modo que $\forall x \in N$,

$$\begin{aligned} f(x) = 0 &\Rightarrow x \text{ es cero o par} \\ f(x) = 1 &\Rightarrow x \text{ es impar.} \end{aligned}$$

Demuéstrese que f es un homomorfismo.

2.586.

Siguiendo los establecimientos anteriores, establézcase el isomorfismo asociado entre las clases homomórficas y $[B, \times]$.

2.587.

Sean $[C, \times]$ y $[R, \times]$ los grupos multiplicativos de los complejos y de los reales, respectivamente. Se crea una aplicación $f: C \to R$, de modo que $\forall(a + bi) \in C$, $f(a + bi) = + (a^2 + b^2)^{1/2} \in R$.

Mostrar que f es un homomorfismo.

2.588.

Demuéstrese que en todo homomorfismo natural entre un grupo y el grupo cociente, módulo un subgrupo invariante suyo, el núcleo coincide con el módulo.

2.589.

Determínese el núcleo del homomorfismo planteado en 2.587.

2.6

Anillos

2.61. Establecimiento de la estructura de anillo

2.62. Anillo de integridad; dominio de integridad

2.621. *Divisores del cero*
2.622. *Anillo de integridad o anillo entero*

2.63. Subanillos

2.631. *Establecimiento*
2.632. *Teorema*

2.64. Homomorfismo en anillos

2.641. *Imagen homomorfa de un anillo* $[A, +, \times]$
2.642. *Núcleo de un homomorfismo entre anillos*

2.65. Ideales

2.651. *Ideal principal*
2.652. *Teorema*
2.653. *El anillo cociente del A, respecto del ideal I*
2.654. *Ideal primo*

2.6541. Teorema
2.6542. Teorema

2.66. Aplicabilidad. Automatismos y destrezas

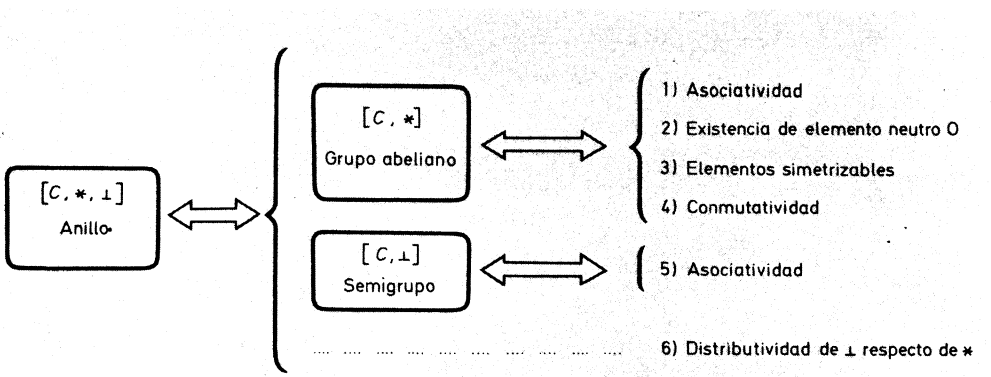
2.6

Anillos

2.61. ESTABLECIMIENTO DE LA ESTRUCTURA DE ANILLO

Siendo el conjunto $C \neq \phi$ y dos leyes de composición interna $*$ y $\perp$, se dice que la terna $[C, *, \perp]$ «es» un anillo si la primera operación $*$ dota a C de estructura de grupo abeliano, la segunda proporciona a C estructura de semigrupo y, además, ésta es distributiva respecto de aquélla.

Esquemáticamente:



Si, como es general, además,

7) Conmutatividad de $\perp$
8) Existencia de elemento unidad 1

entonces se dice que $[C, *, \perp]$ «es» un *ANILLO abeliano con elemento unidad.*

Ejercicio-ejemplo

$[Z, +, \times]$ tiene estructura de anillo abeliano con elemento unidad. Desarróllese.

En lo sucesivo, a la primera operación de un anillo la designaremos por $+$, y la denominaremos *adición*, aun cuando el caso que se trate quede muy lejos de la concreción aritmética elemental que el nombre evoca. Consecuentemente, signaremos por 0 y leeremos «cero» el neutro de esa primera operación; además, la notación genérica para el simétrico de a, que venía siendo a', la sustituiremos por $-a$.

De igual modo, a la segunda operación la llamaremos «multiplicación» o «producto» en todos los casos, y la signaremos indistintamente por los símbolos $\cdot$ o $\times$. En la misma línea, el elemento neutro de esa segunda operación lo llamaremos elemento «unidad» y lo simbolizaremos 1, así como —cuando llegue el caso— el simétrico de un elemento a se denotará a^{-1}.

Semianillo

Algunas veces recibe este nombre una estructura bioperacional con la axiomática del anillo, a excepción del axioma 3). O sea, respecto a la adición, el conjunto estructurado sólo alcanza la estructura de semigrupo abeliano con elemento neutro. El más elemental ejemplo de esta estructura es el ejercicio que se propone.

Ejercicio-ejemplo

$[N \cup \{0\}, +, \times]$ tiene estructura de semianillo abeliano c elemento unidad. Desarróllese.

Consecuencias inmediatas del establecimiento de la estructura de anillo son los tres teoremas elementales que siguen:

TEOREMA 1. Todo elemento del anillo multiplicado por el neutro de la adición es cero. Es decir:

$$\forall a \in C,\ a \cdot 0 = 0 \cdot a = 0$$

En efecto: $b + 0 = 0 + b = b$

$$a \cdot b = a \cdot (b + 0) = (a.\, b) + (a \cdot 0) \Rightarrow a \cdot 0 = 0$$
$$b \cdot a = (b + 0) \cdot a = (b \cdot a) + (0 \cdot a) \Rightarrow 0 \cdot a = 0$$

TEOREMA 2. En todo anillo un elemento multiplicado por el opuesto de otro es igual al opuesto del producto de ambos. O sea:

$$\forall a \in C,\quad \forall b \in C,\quad a \cdot (-b) = -(a \cdot b)$$
$$(-a) \cdot b = -(a \cdot b)$$

En efecto: según el teorema anterior,

$$0 = a \cdot 0 = a \cdot [b + (-b)] = (a \cdot b) + [a \cdot (-b)]$$
$$0 = 0 \cdot b = [a + (-a)] \cdot b = (a \cdot b) + [(-a) \cdot b]$$

Las dos expresiones conseguidas exigen la tesis.

TEOREMA 3. En todo anillo el producto de dos elementos es igual al producto de sus opuestos. Es decir:

$$\forall a \in C, \quad \forall b \in C, \quad a \cdot b = (-a) \cdot (-b)$$

En efecto: aplicando dos veces el teorema anterior,

$$(-a) \cdot (-b) = -[-(-a) \cdot (-b)] = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b$$

La «regla de los signos» en el anillo abeliano con elemento unidad $[Z, +, \times]$.

El tratamiento general que antecede se concreta sobre el cálculo con enteros en las conocidas reglas:

1.ª Todo entero por cero es cero.
2.ª «más» × «menos» = «menos».
«menos» × «más» = «menos».
3.ª «menos» × «menos» = «más».

A2.62. ANILLO DE INTEGRIDAD DOMINIO DE INTEGRIDAD

2.621. Divisores del cero

Se denominan así los elementos no nulos de un anillo cuyo producto es cero. Simbólicamente,

$$a \neq 0, \quad b \neq 0, \quad a \cdot b = 0$$

Ejemplo

En el anillo de las clases residuales, módulo 6 $[\{Z/6\}, +, \times]$, los restos $\bar{3} \in \{Z/6\}$ y $\bar{2} \in \{Z/6\}$ son divisores del cero, ya que $\bar{3} \times \bar{2} = \bar{0}$.

2.622. Anillo de integridad o anillo entero

Se califica así a todo anillo que no tiene divisores del cero. Por tanto, en estos anillos, si el producto de dos elementos es cero, es que al menos uno de los factores es nulo. De este modo:

Si $[C, +, \times]$ es anillo de integridad,

$$a \in C, b \in C, a \cdot b = 0 \Rightarrow \begin{cases} a = 0 \text{ ó} \\ b = 0 \text{ ó} \\ a = b = 0 \end{cases}$$

Si, como es normal, el anillo de integridad tiene elemento unidad, recibe el nombre de *dominio de integridad.*

Ejemplo 1

El anillo de los enteros $[Z, +, \times]$ es un dominio de integridad, porque

a) $a \in Z,\ b \in Z,\ a \cdot b = 0 \Rightarrow \begin{cases} a = 0 \text{ ó} \\ b = 0 \text{ ó} \\ a = b = 0 \end{cases}$

b) Z tiene elemento unidad

$$\forall a \in Z,\ a \cdot (+1) = (+1) \cdot a = a$$

Ejemplo 2

El anillo de las clases residuales, módulo 5 es un dominio de integridad, porque

a) $r_1 \in \{Z/5\},\ r_2 \in \{Z/5\},\ r_1 \cdot r_2 = 0 \Rightarrow \begin{cases} r_1 = 0 \text{ ó} \\ r_2 = 0 \text{ ó} \\ r_1 = r_2 = 0 \end{cases}$

b) $\{Z/5\}$ tiene elemento unidad

$$\forall r \in \{Z/5\},\ r \cdot \bar{1} = \bar{1} \cdot r = r$$

En general, los anillos Z/p, si p es primo, son dominios de integridad, no siéndolo en caso contrario. Esta interesante cuestión se tratará cumplidamente más adelante.

En los anillos (y dominios) de integridad se puede utilizar *la regla de simplificación*, cosa que no es lícita si el anillo tiene divisores del cero.

Sea $[C, +, \times]$ un anillo de integridad y sean a, b y c elementos de él no nulos, de modo que

$$a \times c = b \times c \Rightarrow a \cdot c - b \cdot c = 0 \Rightarrow c \cdot (a - b) = 0$$

Por hipótesis uno de los dos factores, al menos, ha de ser nulo; pero $c \neq 0$, luego

$$a - b = 0 \Rightarrow a = b,$$

resultado que justifica haber simplificado inicialmente la primera expresión

Contraejemplo

Considérese el ya planteado anillo de las clases residuales,

$$\text{módulo } 6\text{: } [\{Z/6\}, +, \times].$$

En este anillo la expresión

$$\bar{x} \cdot \bar{3} = \bar{y} \cdot \bar{3} \not\Rightarrow \bar{x} = \bar{y}$$

es posible que $\bar{x} = \bar{2}$ e $\bar{y} = \bar{4}$ y, sin embargo, se cumple la igualdad

$$\bar{2} \times \bar{3} = \bar{4} \times \bar{3},$$

ya que ambos productos son iguales al residual $\bar{0}$.

Todo ello porque el anillo considerado no es de integridad, por poseer divisores del cero, que son el $\bar{2}$ y el $\bar{3}$.

2.63. SUBANILLOS

2.631. Establecimiento

Un $B \subset C$ es subanillo del anillo $[C, +, \times]$, si $[B, +, \times]$ también tiene estructura de anillo. Por tanto, B habrá de ser:

a) subgrupo aditivo del grupo $[C, +]$
b) semigrupo multiplicativo.

2.632. Teorema

La condición necesaria y suficiente para que un $B \subset C$ sea subanillo del anillo $[C, +, \times]$ es que $\forall a \in B$, $\forall b \in B$,

$$[(a + (-b)) \in B] \wedge [(a \times b) \in B]$$

Para justificar la primera parte de la condición, basta recordar que ésa es precisamente la que se exige para que un subconjunto de un grupo sea subgrupo de él (véase 2.462).

Por lo que se refiere a la segunda parte, entiéndase que de ese modo nos aseguramos que B es semigrupo multiplicativo, conservándose —por supuesto— la asociatividad del semigrupo $[C, \times]$.

Además, es inmediato comprobar que la distributividad multiplicativa sobre la adición se mantiene.

Ejemplo

Se considera del anillo de los enteros, el subconjunto $B = \{x/(x \in Z) \wedge (x = \dot{5})\}$. B es un subanillo de Z. Efectivamente: $\forall a \in B$, $\forall b \in B$, se cumple el teorema anterior,

$$a + (-b) = 5p + (-5q) = 5(p - q) \in B$$
$$a \times b = (5p \times 5q) \in B$$

Observación. Conviene evitar el posible error de suponer que todo subanillo de un anillo ha de conservar las características de éste. Por ejemplo, no se puede asegurar que un subanillo de un dominio de integridad lo siga siendo; aún más: puede suceder que de un anillo con elemento unidad se obtenga un subanillo sin este elemento, e incluso, que lo tenga distinto.

En el ejemplo anterior se ha cuidado de presentar un subanillo del dominio de

integridad de los enteros que «ha perdido» el elemento unidad. Efectivamente, $1 \notin B$.

2.64. HOMOMORFISMO EN ANILLOS

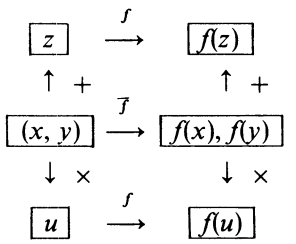
Se establecen los anillos $[A, +, \times]$ y $[B, +, \times]$.

Extendiendo el concepto de homomorfismo entre grupos (número 2.51) a esta estructura bioperacional, se dirá que una aplicación f entre los anillos establecidos es homomorfismo, si se verifica:

$$x + y = z \Rightarrow f(x) + f(y) = f(z)$$
$$x \cdot y = u \Rightarrow f(x) \cdot f(y) = f(u),$$

siendo u, z, x e y elementos del anillo A.

Tal vez este esquema sirva de ayuda para fijar el concepto, al igual que se hizo en Grupos.



Ejemplo

1.º Se establece el conjunto de todos los polinomios monoindeterminados de coeficientes reales, $P(x)$; y sobre él, las conocidas operaciones de adición y multiplicación de polinomios. Queda así creado el anillo abeliano con elemento unidad de los polinomios $[P(x), +, \times]$.

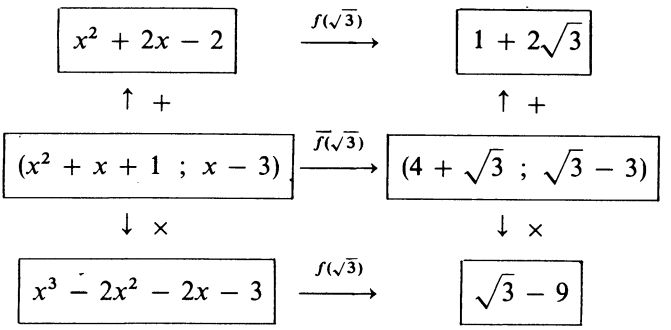
2.º Se establece ahora el subconjunto de los reales $P(a)$, cuyos elementos son los valores numéricos de los polinomios de $P(x)$, $\forall a \in R$. Este conjunto con las operaciones de adición y multiplicación en R, es un anillo abeliano con elemento unidad y con elementos inversibles en la multiplicación, a excepción del cero (es decir, un cuerpo):

$$[P(a), +, \times]$$

3.º A cada polinomio se hace corresponder su valor numérico, quedando así una aplicación f entre ambos anillos, que es un homomorfismo

$$[P(x), +, \times] \xrightarrow{f} [P(a), +, \times].$$

Veamos una particularización:



Toda la nomenclatura que, en Grupos, se estableció para homomorfismos (número 2.54) se traslada a la cuestión, referida a anillos.

2.641. Imagen homomorfa de un anillo $[A, +, \times]$

Es improcedente repetir aquí el establecimiento del concepto, así como los teoremas inmediatos, a él referibles, puesto que se trata de una simple extrapolación de la teoría expuesta en el número 2.52, para Grupos. Sin embargo, no deja de ser cómodo tener registrados aquí los escuetos enunciados de la cuestión tratada:

TEOREMA. La imagen homomorfa de cualquier subanillo de $[A, +, \times]$, mediante f, en $[B, +, \times]$ es —al menos— un subanillo de B.

COROLARIO. La imagen homomorfa de $[A, +, \times]$ en $[B, +, \times]$, mediante el homomorfismo f, es un subanillo de B.

TEOREMA. La imagen recíproca de todo subanillo de B es un subanillo de A.

TEOREMA. La imagen del neutro (aditivo) de $[A, +, \times]$ es el neutro (aditivo) de $[B, +, \times]$.

TEOREMA. La imagen del opuesto de $x \in A$ es el simétrico de su imagen, $f(x) \in B$.

2.642. Núcleo de un homomorfismo entre anillos

El núcleo de un homomorfismo entre anillos es exactamente el mismo concepto que en el número 2.56 se estableció entre grupos. Es decir, en el homomorfismo entre anillos

$$[A, +, \times] \xrightarrow{f} [B, +, \times],$$

$$\ker(f) \equiv A_1 \subset A / \forall x \in A_1, f(x) = 0$$

(Denotamos por 0 el neutro aditivo del grupo $[B, +]$.)

Recordemos también estos dos establecimientos, ya justificados:

1.º $\ker(f)$ es subgrupo aditivo de A.

2.º $\ker(f)$ es subgrupo normal de A (puesto que $[A, +]$ es abeliano).

Todo ello nos permite abordar ahora el siguiente

TEOREMA. El núcleo de un homomorfismo entre anillos $[A, +, \times]$ y $[B, +, \times]$ es subanillo de A.

Para demostrarlo, bastará comprobar que se cumplen las dos condiciones que se exigen para que un $A_1 \subset A$ sea subanillo de A.

1.ª $\forall a \in \ker(f)$, $\forall b \in \ker(f)$, $a + (-b) \in \ker(f)$
En efecto, ya que $\ker(f)$ es subgrupo de A;

2.ª $a \times b \in \ker(f)$
En efecto:

$$f(a \cdot b) = f(a) \cdot f(b)$$
$$f(a) \cdot f(b) = 0 \cdot 0 = 0$$
$$f(a \cdot b) = 0 \Rightarrow (a \cdot b) \in \ker(f)$$

Tras desarrollar el siguiente epígrafe, volveremos sobre el núcleo de un homomorfismo entre anillos, para ver que el $\ker(f)$ es «bastante más» que subanillo de A.

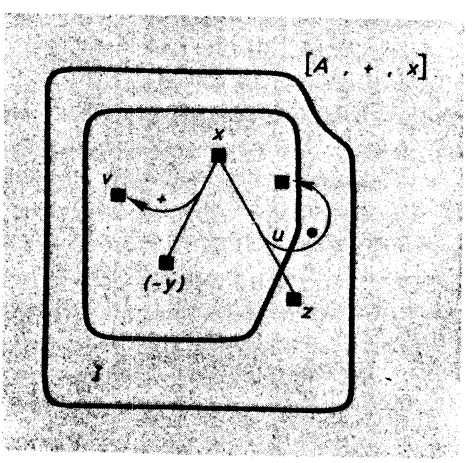
2.65. IDEALES

Sea I un subconjunto del anillo $[A, +, \times]$, que llega a ser subanillo de A.

Pero, además, tiene la particularidad de que el producto de cualquier $x \in I$ por un $z \in A$ es un elemento de I

$$x \cdot z = u$$

A tales subconjuntos I se les denomina ideales de A.



Así, pues, se define*.

$$\left.\begin{array}{l} I \subset A \text{ es ideal de} \\ [A, +, \times] \end{array}\right\} \Leftrightarrow \left\{\begin{array}{ll} 1.^{o} & \forall x \in I,\ \forall y \in I,\ x + (-y) = v \in I \\ 2.^{o} & \forall x \in I,\ (z \in A) \rightarrow x \cdot z = u \in I \end{array}\right.$$

2.651. Ideal principal

Cuando todos y cada uno de los elementos de una ideal se generan mediante el producto de un elemento fijo del anillo por otros de él, se dice que es un ideal principal. Simbólicamente:

$$\left.\begin{array}{l} I \text{ es ideal} \\ \text{principal de } A \end{array}\right\} \Leftrightarrow \forall x \in I,\ \exists^{*} a \in A / x = y \cdot a\ \ (y \in A)$$

El elemento a recibe el nombre de generador o base de I.

2.652. Teorema

El $\ker(f)$ de un homomorfismo entre anillos es ideal del anillo original.

El teorema del número 2.642 concluía que el núcleo es subanillo de A; queda aquí, pues, solamente justificar que

$$\forall a \in \ker(f),\ (c \in A) \rightarrow (a \cdot c) \in \ker(f)$$

En efecto:

$$f(a \cdot c) = f(a) \cdot f(c) = 0 \cdot f(c) = 0$$

(Se ha denotado 0 el neutro de $[B, +]$.)

$$f(a \cdot c) = 0 \Rightarrow a \cdot c \in \ker(f)$$

2.653. El anillo cociente del A, respecto del ideal I

En la definición de ideal queda establecido que I es un subgrupo normal o invariante de A. De modo que el conjunto-cociente A/I se estructura en forma de grupo-cociente por la adición inducida entre sus clases (véase número 2.485).

Se establecerá a continuación que A/I alcanza la estructura de semigrupo multiplicativo abeliano con elemento unidad (si A era conmutativo y tenía elemento unidad) mediante la multiplicación inducida entre sus clases.

0) Sea el anillo abeliano con elemento unidad $[A, +, \times]$, e I un ideal suyo.

---

* La definición que se establece es la de ideal por la derecha. Si para la 2.ª condición esencial se escribiera $z \cdot x = u$, se definiría un ideal por la izquierda.

Si, como es frecuente, se trata de anillos abelianos, al ser conmutativa la multiplicación, no existe diferencia entre ambas expresiones, siendo en este caso los ideales «biláteros».

1) Se crea el grupo-cociente aditivo $[A/I, +]$ mediante la adición inducida entre sus clases, que se establece:

$$\{(x + I)\} \hat{+} \{(y + I)\} = \{(a + b) + I\} \quad \text{(véase 2.485)}$$

2) Se crea el semigrupo multiplicativo abeliano con elemento unidad $[A/I, \bar{\times}]$.

2*a*) Se establece la multiplicación inducida entre las clases de A/I, de este modo:

$$\{(x + I)\} \bar{\times} \{(y + I)\} = \{(x \cdot y) + I\}$$

2*b*) Análisis de la operación

$2b_1$) La multiplicación entre clases es operación (= ley de composición interna), ya que, como $(x \cdot y) \in I$, la clase-resultado $\{(x \cdot y) + I\} \in A/I$

$2b_2$) Es uniforme.
Para demostrarlo, basta probar que es estable frente a la relación de equivalencia que definió las clases. O lo que es igual: que la clase-resultado no depende de los representantes de las clases-operando, escogidos para operar.
Establezcamos las clases $\{x + I\} = \{(x + m), (x + n), \ldots\}$
y $\{y + I\} = \{(y + m), (y + n), \ldots\}$
Operemos esas clases usando unos de sus representantes:

$$\{x + I\} \bar{\times} \{y + I\} = (x + m) \bar{\times} (y + m) = \{(x \cdot y) + m\}.$$

y ahora hagámoslo usando otros representantes:

$$\{x + I) \bar{\times} \{y + I\} = (x + n) \bar{\times} (y + n) = \{(x \cdot y) + n\}.$$

Ambos resultados obtenidos pertenecen a la misma clase $\{(x \cdot y) + I\}$, órbita del elemento $(x \cdot y) \in A$; de modo que la clase-resultado no depende de los representantes escogidos como operandos, c.q.d.

$2b_3$) Es asociativa

$$\{x + I\} \bar{\times} [(y + I) \bar{\times} (z + I)] = (x + I) \bar{\times} [(y \cdot z) + I] =$$
$$= \{x \cdot (y \cdot z) + I\} = \{(x \cdot y) \cdot z + I\} = \{(x \cdot y) + I\} \bar{\times} (z + I) =$$
$$= [(x + I) \bar{\times} (y + I)] \bar{\times} (z + I)$$

$2b_4$) Tiene clase-unidad.
Siendo 1 el elemento unidad de A, la clase $\{1 + I\}$ es precisamente la clase-unidad del semigrupo $[A/I, \times]$. En efecto: sea una clase $\{x + I\} \in A/I$:

$$\{x + I\} \bar{\times} \{1 + I\} = \{(x \cdot 1) + I\} = \{x + I\}; \text{ y también,}$$
$$\{1 + I\} \bar{\times} \{x + I\} = \{(1 \cdot x) + I\} = \{x + I\}$$

$2b_5$) Es conmutativa
De justificación inmediata.

3) La multiplicación entre clases de A/I es distributiva respecto de la adición. En efecto:

$$\{x + I\} \bar{\times} [\{y + I\} \tilde{+} \{z + I\}] = \{x + I\} \bar{\times} [\{(y + z) + I\}] =$$
$$= \{[x \cdot (y + z)] + I\} = \{[(x \cdot y) + (x \cdot z)] + I\} =$$
$$= \{(x \cdot y) + I\} \tilde{+} \{(x \cdot z) + I\} =$$
$$= \{x + I\} \bar{\times} \{y + I\} \tilde{+} \{x + I\} \bar{\times} \{z + I\}$$

4) Conclusión: El conjunto-cociente, respecto del ideal I, $\{A/I\}$, ha quedado estructurado —a su vez— como anillo abeliano con elemento unidad. Al anillo cociente $[\{A/I\}, +, \times]$ se le suele denominar anillo de clases residuales, módulo I*.

2.654. Ideal primo

Sea el anillo abeliano con elemento unidad $[A, +, \times]$, e I un ideal suyo.

Se dirá que I es ideal primo de A si, perteneciendo a él el producto de dos elementos de A, los factores-operandos son los dos elementos de I o, al menos, uno de ellos. Consecuentemente, en este caso, el anillo cociente A/I siempre es de integridad.

Simbólicamente:

$$\left.\begin{array}{l}\text{es ideal primo}\\ \text{de } [A, +, \times]\end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} x \in A \quad , \quad y \in A \\ x \cdot y = z \in I \Rightarrow (x \vee y) \in I\end{array}\right.$$

(Recuérdese que la disyunción no exclusiva $\vee$ es o/y.)

Ejemplo 1

En el anillo abeliano con elemento unidad de los enteros $[Z, +, \times]$ se considera el subconjunto $\{\dot{5}\}$ de los múltiplos de 5.

— Compruébese que, en efecto, $\{\dot{5}\}$ es un subanillo de Z;
— que es «más que subanillo»: es un ideal de Z;
— que es un ideal primo.

Ejemplo 2

En $[Z, +, \times]$ considérese el subconjunto $\{\dot{6}\}$ de los múltiplos de 6.

— Compruébese que $\{\dot{6}\}$ es un subanillo de Z;
— que llega a ser un ideal de Z;
— que es un ideal no primo.

En el ejemplo 1, si $a \cdot b \in \{\dot{5}\}$ es porque a, b o uno de los dos son múltiplos de

---

* A partir de ahora, denotaremos indistintamente las operaciones genéricas del anillo A y las inducidas en sus anillos-cociente por los signos convencionales $+$ y $\times$. Hasta aquí, se ha mantenido —laboriosamente— distinta tipografía para las leyes inducidas, con clara intencionalidad didáctica.

cinco; en el ejemplo 2, el que $a \cdot b \in \{\dot{6}\}$, no implica que lo sea alguno(s) de los dos factores; por ejemplo,

$$4 \times 9 = 36,$$

y, ni 4 ni 9 son múltiplos de 6.

2.6541. TEOREMA

La condición necesaria y suficiente para que un anillo-cociente A/I sea dominio de integridad es que el ideal I sea primo.

T_1) *Condición necesaria*

H. I es primo; o sea: siendo I el neutro de $[A/I, +]$,

$$\{x + I\} \cdot \{y + I\} = I, \{x + I\} \neq I$$

T. $\{y + I\} = I$

D. $\{x + I\} \cdot \{y + I\} = \{(x \cdot y) + I\} = I \Rightarrow x \cdot y \in I$ [1]

$$\{x + I\} \neq I \Rightarrow x \notin I \quad [2]$$

Pero como I es primo, la única manera de que se cumplan [1] y [2] es que $y \in I \Rightarrow \{y + I\} = I$.

T_2) *Condición suficiente*

H. A/I es anillo de integridad; o sea:

$$x \cdot y \in I, \; x \notin I$$

T. $y \in I$

D. $x \cdot y \in I \Rightarrow \{(x \cdot y) + I\} = \{x + I\} \cdot \{y + I\} = I$ [3]

$$x \notin I \Rightarrow \{x + I\} \neq I \quad [4]$$

Pero como A/I es anillo de integridad, según [3] y [4] se cumple que $\{y + I\} = I \Rightarrow y \in I$.

2.6542. TEOREMA

La aplicación del anillo A en uno de sus anillos cociente A/I, que hace corresponder a cada $x \in A$ su clase $\{x + I\} \in A/I$, es un homomorfismo cuyo núcleo es el ideal I.

$$[A, +, \times] \xrightarrow{\Phi} [A/I, +, \times]$$
$$x \to \Phi(x) \equiv \{x + I\}$$

La aplicación Φ es un homomorfismo. En efecto:

$$x + y = z$$
$$\Phi(x) + \Phi(y) = \{x + I\} + \{y + I\} =$$
$$= \{(x + y) + I\} =$$
$$= \{z + I\} \equiv \Phi(z)$$

$$x \cdot y = u$$
$$\Phi(x) \cdot \Phi(y) = \{x + I\} \cdot \{y + I\} =$$
$$= \{(x \cdot y) + I\} =$$
$$= \{u + I\} \equiv \Phi(u)$$

El núcleo es I. Veamos:
La clase neutra de A/I es precisamente $\{I\}$.

$$x \cdot y \in \ker(\Phi) \Rightarrow \Phi(x \cdot y) = \Phi(x) \cdot \Phi(y) = \{I\};$$
$$\{x + I\} \cdot \{y + I\} = \{I\};$$
$$\{(x \cdot y) + I\} = \{I\} \Rightarrow (x \cdot y) \in I;$$
$$\ker(\Phi) \equiv I$$

2.66. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

2.660.
Resuélvase justificadamente (si procede) en el anillo de los enteros la ecuación

$$a \cdot x + b = c$$

(No se omita ningún paso, ni la base axiomática de cada uno de ellos.)

2.661.
En el anillo de las clases residuales, módulo 5, resuélvase la ecuación

$$3x + 2 = 1,$$

en la que tanto los coeficientes como la incógnita son restos del anillo establecido. (Constrúyanse las tablas, previamente.)

2.662.
En el anillo de las clases residuales, módulo 6, resuélvase el sistema

$$\begin{array}{ll} \text{I} & x + y = 3 \\ \text{II} & 2x - 3y = 1, \end{array}$$

en el que tanto los coeficientes como las incógnitas son clases residuales del anillo establecido que, por cierto, no es de integridad.

(Establézcanse las tablas de las dos operaciones; descríbanse los divisores del cero. Recuérdese que no es posible simplificar.)

2.663.
Resuélvase en el anillo $Z/5$ la ecuación cuadrática

$$x^2 - 3x + 1 = 0$$

2.664.

Justifíquese que todo ideal del anillo de los enteros es principal.

2.665.

Justifíquese que todo ideal que contenga el elemento unidad del anillo A coincide con el propio A.

2.666.

Siendo I_1 e I_2 dos ideales del anillo abeliano A, se define adición de ideales de este modo:

$$I_1 + I_2 = I_3$$
$$\forall x \in I_1, \quad \forall y \in I_2, \quad \exists z \in I_3 / x + y = z$$

Justifíquese que la ley establecida es cerrada en el conjunto de ideales de A.

2.667.

Establézcase el concepto de máximo común divisor de dos enteros, usando la teoría de adición de ideales en Z.

2.668.

Siendo I_1 e I_2 dos ideales del anillo abeliano A, se define intersección de ideales de la siguiente manera:

$$[I_1, +, \times] \cap [I_2, +, \times] = [(I_1 \cap I_2), +, \times]$$

Demuéstrese que la operación establecida es cerrada en el conjunto de ideales de A.

2.669.

Establézcase el concepto de mínimo común múltiplo de dos enteros usando la teoría de la intersección de ideales en Z.

2.7

Cuerpos

2.71. Establecimiento de la estructura de cuerpo

2.72. Creación de cuerpos: simetrización en dominios de integridad

2.721. *El semigrupo a simetrizar*
2.722. *El cuerpo de fracciones de un dominio de integridad*
2.723. *El dominio de integridad sumergido en el cuerpo creado*
2.724. *Un ejemplo importante: el cuerpo de los complejos*

2.73. Subcuerpos

2.731. *Establecimiento*
2.732. *Teorema*
2.733. *Característica de un cuerpo. Cuerpo primo*

2.74. Ordenación en grupos, anillos y cuerpos

2.741. *Grupo ordenado*

2.7411. Cono positivo de un grupo ordenado

2.742. *Anillo ordenado*

2.7421. Regla de los signos

2.743. *Cuerpo ordenado*
2.744. *Ordenes arquimedianos*

2.75. Aplicabilidad. Automatismos y destrezas

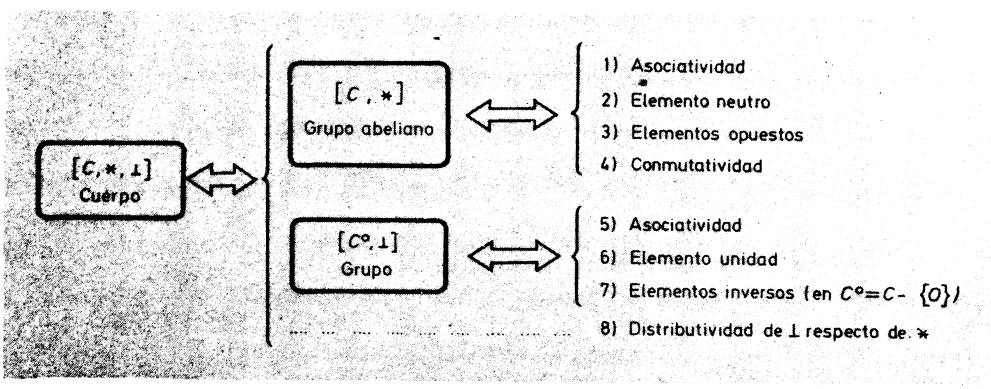
2.7

Cuerpos

2.71. ESTABLECIMIENTO DE LA ESTRUCTURA DE CUERPO

Siendo el conjunto $C \neq \phi$ y dos leyes de composición interna $*$ y $\perp$, se dice que la terna $[C, *, \perp]$ «es» un cuerpo si alcanza estructura de anillo con elemento unidad y, además, todos los elementos de C, a excepción del neutro de la primera ley, son inversibles.

Esquemáticamente:



Si, como es frecuente, la operación segunda $\perp$, es conmutativa, $[C, *, \perp]$ alcanza la estructura de CUERPO ABELIANO.

Resultando ser un cuerpo un anillo con «mayor exigencia estructural», es evidente que toda la teoremática de anillos es trasladable, completa, a los cuerpos.

Siendo lo general tratar de cuerpos sobre un conjunto C que no posee divisores del cero, los cuerpos, entonces, son dominios de integridad, puesto que poseen elemento unidad: toda la teoría, pues, de los dominios de integridad es aplicable a los cuerpos.

A partir de aquí —e igual que hicimos en anillos— usaremos los signos + y × para simbolizar la 1.ª y la 2.ª operación del cuerpo, que denominaremos en todos los casos adición y multiplicación.

2.72. CREACION DE CUERPOS: SIMETRIZACION EN DOMINIOS DE INTEGRIDAD

En el epígrafe 2.432 quedaba desarrollada cumplidamente la simetrización de semigrupos. Es, punto por punto, lo que ha de hacerse aquí con el semigrupo multiplicativo del dominio.

2.721. El semigrupo a simetrizar

Disponemos del anillo abeliano con elemento unidad, cancelativo (= sin divisores del cero), es decir, del dominio de integridad $[A, +, \times]$, y en él, del semigrupo multiplicativo abeliano con elemento unidad $[A, \times]$.

Se construye el cartesiano $A \times A^0$, en el que A^0 representa el conjunto A, privado de elemento neutro de la adición.

Se establece una relación de equivalencia R sobre $A \times A^0$:

$$\forall (a, b) \in A \times A^0, \quad \forall (c, d) \in A \times A^0,$$
$$(a, b) \equiv (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

El análisis de R, realizado en 2.4322, la justifica como relación de equivalencia. Al actuar sobre $A \times A^0$, clasifica y parte a ese cartesiano en clases de equivalencia, formando el conjunto cociente $C = A \times A^0/R$.

2.722. El cuerpo de fracciones de un dominio de integridad

A) La ley producto en A es estable frente a la relación de equivalencia R, que define C a partir de $A \times A^0$. Se induce una ley multiplicación entre las clases de C^0 que le estructura en forma de grupo (siga consultándose el 2.4322)*.

$$\forall \{a, b\} \in C^0, \quad \forall \{c, d\} \in C^0,$$
$$\{a, b\} \times \{c, d\} = \{a \cdot c, b \cdot d\}$$

---

* Adviértase que la multiplicación actúa sobre $C^0 = C - \{0\}$ y no sobre C. Es necesario prescindir de la clase cero, para que, siendo inversibles todos los elementos, $[C^0 \cdot \times]$ sea grupo.

B) Por lo que se refiere a la adición, a partir del grupo abeliano $[A; +]$, se induce entre las clases de C la siguiente operación:

$$\forall\{a, b\} \in C, \quad \forall\{c, d\} \in C$$
$$\{a, b\} + \{c, d\} = \{(a \cdot d + b \cdot c), (b \cdot d)\}$$

Se ha de justificar ahora que $[C, +]$ es un grupo abeliano:

B_1) La adición establecida entre las clases de C es uniforme por ser estable frente a la relación R que creó C, a partir de $A \times A^0$. Basta para probarlo justificar que el resultado de operar dos clases no depende de los representantes escogidos como operandos.

(Usaremos el más cómodo formalismo de las fracciones, en lugar del de los pares.)

Sean dos clases de C:

$$\{\alpha\} \equiv \left\{ \frac{a_1}{b_1} \equiv \frac{a_2}{b_2} \equiv \cdots \right\} \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1$$

$$\{\beta\} \equiv \left\{ \frac{c_1}{d_1} \equiv \frac{c_2}{d_2} \equiv \ldots \right\} \Leftrightarrow c_1 \cdot d_2 = c_2 \cdot d_1$$

Multiplicando la primera expresión por $d_1 \cdot d_2$ y la segunda por $b_1 \cdot b_2$, se obtiene:

$$\left.\begin{array}{l} a_1 \cdot b_2 \cdot d_1 \cdot d_2 = a_2 \cdot b_1 \cdot d_1 \cdot d_2 \\ c_1 \cdot d_2 \cdot b_1 \cdot b_2 = c_2 \cdot d_1 \cdot b_1 \cdot b_2 \end{array}\right\} +$$

$$b_2 \cdot d_2 \cdot (a_1 \cdot d_1 + c_1 \cdot b_1) = b_1 \cdot d_1 \cdot (a_2 \cdot d_2 + c_2 \cdot b_2)$$

$$\frac{a_1 \cdot d_1 + c_1 \cdot b_1}{b_1 \cdot d_1} \Updownarrow \frac{a_2 \cdot d_2 + c_2 \cdot b_2}{b_2 \cdot d_2}$$

$$\left\{\frac{a_1}{b_1}\right\} + \left\{\frac{c_1}{d_1}\right\} = \left\{\frac{a_2}{b_2}\right\} + \left\{\frac{c_2}{b_2}\right\}$$

B_2) Se prueba muy fácilmente que $[C, +]$ goza de asociatividad.

B_3) Existencia de elemento neutro

$$\forall \left\{\frac{a}{b}\right\} \in C, \exists^* \left\{\frac{0}{m}\right\} \in C / \left\{\frac{a}{b}\right\} + \left\{\frac{0}{m}\right\} = \left\{\frac{0}{m}\right\} + \left\{\frac{a}{b}\right\} = \left\{\frac{a}{b}\right\}$$

Basta operar para comprobarlo.

B_4) Elementos opuestos

Es obvio que $\forall \left\{\frac{a}{b}\right\} \in C$, su clase opuesta es $\left\{\frac{-a}{b}\right\}$

Justifíquese.

C) La multiplicación en C es distributiva respecto de la adición

$$\left[\left\{\frac{a}{b}\right\} + \left\{\frac{c}{d}\right\}\right] \times \left\{\frac{e}{f}\right\} = \left\{\frac{a \cdot d + b \cdot c}{b \cdot d}\right\} \times \left\{\frac{e}{f}\right\} = \left\{\frac{a \cdot d \cdot e + b \cdot c \cdot e}{b \cdot d \cdot f}\right\} =$$

$$= \left\{\frac{a}{b}\right\} \times \left\{\frac{e}{f}\right\} + \left\{\frac{c}{d}\right\} \times \left\{\frac{e}{f}\right\} = \left\{\frac{a \cdot e}{b \cdot f}\right\} + \left\{\frac{c \cdot e}{d \cdot f}\right\} = \left\{\frac{a \cdot e \cdot d \cdot f + c \cdot e \cdot b \cdot f}{b \cdot f \cdot d \cdot f}\right\} =$$
$$= \left\{\frac{a}{b}\right\} \times \left\{\frac{e}{f}\right\} + \left\{\frac{c}{d}\right\} \times \left\{\frac{e}{f}\right\}$$

Queda establecido así el cuerpo de fracciones del anillo de integridad, A.

Ejercicio-Ejemplo

Constrúyase el cuerpo de los números racionales, Q, como cuerpo de fracciones del dominio de integridad de los enteros, Z.

2.723. El dominio de integridad sumergido en el cuerpo creado

En el número 2.57 se establecían dos ejemplos que allí quedaron incompletos por referirse a «inmersiones» de estructuras parciales monooperacionales; quiere decirse que se hablaba de inmersión de Z en Q, pero solamente desde el punto de vista del semigrupo multiplicativo $[Z, \times]$ y del grupo multiplicativo $[Q^\circ, \times]$.

Ahora se puede tratar esta cuestión a plenitud, considerando las estructuras completas bioperacionales: el dominio de integridad $[Z, +, \times]$ y el cuerpo $[Q, +, \times]$.

Centrados en el ejemplo recordatorio, se pasa a desarrollar la cuestión general.

1. Se establece la aplicación f entre el dominio de integridad A y el cuerpo de sus fracciones C, cuyo criterio es

$$[A, +, \times] \xrightarrow{f} [C, +, \times]$$
$$a \longrightarrow f(a) = \left\{\frac{a \cdot x}{x}\right\} \quad (\text{para } x \in A^0)$$

(Que $\left\{\frac{a \cdot x}{x}\right\}$, o como allí se decía $\{a \cdot x, x\}$, es una clase de $C = A \times A^0/R$ quedó justificado en 2.57.)

2. La aplicación f, obviamente, es un homomorfismo inyectivo multiplicativo, es decir, un monomorfismo entre $[A, \times]$ y $[C^0, \times]$.

Si se restringe el monomorfismo f al subconjunto de C^0, formado por las imágenes de A, aparece un monomorfismo epimórfico, o sea, un isomorfismo.

3. La aplicación f es un monomorfismo aditivo entre $[A, +]$ y $[C, +]$. Para justificarlo, veamos primero que es homomorfismo, y luego que es inyectivo:

3.1. $$\left\{\frac{a \cdot x}{x}\right\} + \left\{\frac{b \cdot y}{y}\right\} = \left\{\frac{a \cdot x \cdot y + x \cdot b \cdot y}{x \cdot y}\right\} = \left\{\frac{(a + b) \cdot x \cdot y}{x \cdot y}\right\} =$$
$$= \left\{\frac{c \cdot (x \cdot y)}{(x \cdot y)}\right\}$$
$$\forall a \in A, \quad \forall b \in A, \quad a + b = c, \quad c \in A;$$

es decir:

$$f(a) + f(b) = f(c)$$

3.2. Se comprueba ahora que cumple el teorema 2.563, que exige que el núcleo ha de ser unitario para que el homomorfismo sea inyectivo: $\ker(f) \equiv \{0\}$.

Sea un $a \in \ker(f)$ y sea $\left\{\frac{0}{m}\right\} \in C$, el neutro aditivo del cuerpo de fracciones. Entonces

$$\left\{\frac{a \cdot x}{x}\right\} \equiv \left\{\frac{0}{m}\right\} \Leftrightarrow a \cdot x \cdot m = x \cdot 0$$

Por ser A de integridad, admite la simplificación (ley cancelativa)

$$a \cdot m = 0;$$

pero, siendo $m \neq 0$,

$$a = 0;$$

es decir:

$$\ker(f) \equiv \{0\}, \quad \text{c.q.d.}$$

Si se restringe el monomorfismo f al subconjunto de C^0, formado por las imágenes de A, se obtiene una f exhaustiva: un isomorfismo.

De este modo, se puede decir de alguna manera que el cuerpo creado ha captado al dominio que lo generó. A eso se refiere el vulgarismo $Z \subset Q$ y, en general, $A \subset C$.

En realidad, lo que sucede es que se asimila el dominio de integridad A al subconjunto de C, imagen suya, en el isomorfismo que hemos venido estableciendo.

2.724. Un ejemplo importante: el cuerpo de los complejos

No cause extrañeza que aparezca aquí el cuerpo de los complejos, sin referencias previas al cuerpo de los reales, en el cual se fundamenta.

Entendemos que el lector, a nivel elemental, se ha enfrentado ya con una introducción al número real o —cuando menos— estamos convencidos de que su uso le es familiar.

Hemos preferido dejar el tratamiento de los reales, íntegro, para la sección de Análisis del libro. Allí, sin ninguna restricción, lo propiamente algebraico, junto con lo topológico, aunándose, dan toda la medida de tan importante campo.

Sea $R(x)$ el dominio de integridad de los polinomios monoindeterminados de coeficientes reales; y sea también el $(x^2 + 1) \in R(x)$.

El conjunto de todos sus múltiplos $(x^2 + 1) \cdot p(x)$ constituye un ideal de $R(x)$, tal como se vio en la teoría de ideales:

$$I \equiv \{\overline{x^2 + 1}\}$$

Se construye el anillo-cociente, módulo I,

$$C = R(x)/I,$$

cada una de cuyas clases, $\{p(x) + I\}$ está formada por todos los polinomios que dan al mismo resto, al dividirlos por $x^2 + 1$.

(Consúltese, si es necesario, el ejemplo del 2.48.)

Los polinomios

$$\begin{aligned} p_1(x) &= x^3 + 3x + 3 \\ p_2(x) &= -x^3 + x^2 + x + 4 \\ p_3(x) &= x^4 + 2x + 4 \\ p_4(x) &= 2x + 3, \end{aligned}$$

pertenecen todos a la misma clase, porque todos dan de resto $3 + 2x$, al dividirlos por $x^2 + 1$.

Se trata ahora de tomar para las clases de $R(x)/I$ los representantes más sencillos. Obviamente, el representante más sencillo de cada clase será el propio resto, común a todos los polinomios de ella.

Como el divisor, $x^2 + 1$ es de segundo grado, el polinomio-resto es lineal, de la forma $a + bx$, de modo que las clases de C toman la forma canónica

$$\{(a + bx) + I\} \qquad [1]$$

En nuestro ejemplo, la clase de C se escribiría así:

$$\{(3 + 2x) + I\}$$

Resultando sumamente engorroso todo tratamiento de complejos, al arrastrar los formalismos de notación, que nacen de su creación estructural como clases, módulo el ideal $\{\overline{x^2 + 1}\}$, es muy conveniente, antes de seguir adelante, adoptar las simplificaciones de escritura consagradas por el uso; pero no es menos cierto que, si esta adopción no se realiza cuidadosamente, el lector puede perder «de golpe» todo nexo de la base estructural que se viene estableciendo con la «típica cara operativa» de los complejos, resultando la tan frecuente como indeseable «artesanía matemática», divorciada de toda base estructural y huérfana de ciencia.

Consecuentes con lo escrito, no nos importa extendernos en estos puntos:

a) Una de las clases de C estará constituida por los polinomios de grado 0, del tipo

$$ax^0 + 0x^1 + 0x^2 + \ldots$$

Estos polinomios darán de resto a, al dividirlos por $x^2 + 1$ y, por tanto, su clase será

$$\{a + I\} \qquad [2]$$

b) Otra clase de C será la formada por los polinomios del tipo

$$0x^0 + bx^1 + 0x^2 + \ldots ;$$

dando de resto, al dividirlos por $x^2 + 1$, el polinomio bx, su clase tomaría la forma

$$\{bx + I\} \qquad [3]$$

Establecido justificadamente el conjunto-cociente $R(x)/I$ como anillo, están formalizadas tanto la adición como la multiplicación de clases, tal como se hizo en el capítulo anterior. De modo que:

$$\{bx + I\} = \{b + I\} \cdot \{x + I\} \qquad [4]$$

c) Resulta elemental establecer un isomorfismo de R en el subconjunto de C, formado por todas las clases polinómicas de grado cero:

$$\begin{array}{l} R \overset{f}{\longrightarrow} C_0 \\ a \longrightarrow f(a) \equiv \{a + I\} \\ b \longrightarrow f(b) \equiv \{b + I\} \end{array}$$

d) Queda solamente establecer un convenio de simbología, vacío absolutamente de todo contenido matemático; es éste: a las clases del tipo $\{x + I\}$ les signaremos por la letra i.

Usando todo lo dicho, procedemos a sumar las clases [2] y [3], resultándonos la clase «general» [5]

$$\{(a + bx) + I\} = \{a + I\} + \{bx + I\} \qquad [5]$$

Sustituyamos [4] en [5]

$$\{(a + bx) + I\} = \{a + I\} + \{b + I\} \cdot \{x + I\}$$

Finalmente, usando *c*) y *d*), hemos llegado a la notación simplista de los complejos, traducción lícita de la enojosa notación estructural con que nacieron:

$$\{(a + bx) + I\} = \{a + I\} + \{b + I\} \cdot \{x + I\} = a + bi$$

En el ejemplo que venimos intercalando

$$\{(3 + 2x) + I\} = (3 + 2i)$$

Establecido el anillo cociente $R(x)/I$ de los complejos como anillo abeliano con elemento unidad*, ha de demostrarse que llega a ser cuerpo, justificándose que todos sus elementos, excepto el cero, tienen inverso.

---

* Aconsejamos al lector el espléndido ejercicio de explicitar todos y cada uno de los axiomas de la estructura, estableciendo la adición y multiplicación de complejos y describiendo la clase cero, la clase unidad y las clases opuestas.

Dejado al cuidado del lector, éste habrá de conseguir $\forall(a + bi) \neq 0$,

$$(a + bi)^{-1} = \left(\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i\right)$$

Para ello —y así terminamos— dispondrá convenientemente justificada, de la igualdad básica del cálculo de complejos: $i^2 = -1$.

Veamos: el neutro aditivo en los anillos-cociente es el propio ideal que los genera,

$$\{(x^2 + 1) + I\} \equiv I \equiv 0,$$

de modo que:

$$i^2 + 1 = i \cdot i + 1 = \{x + I\} \cdot \{x + I\} + \{1 + I\} = \{(x \cdot x) + I\} + \{1 + I\} =$$
$$= \{x^2 + I\} + \{1 + I\} = \{(x^2 + 1) + I\} = 0$$

2.73. SUBCUERPOS

2.731. Establecimiento

Un $B \subset C$ es subcuerpo del cuerpo $[C, +, \times]$ si $[B, +, \times]$ también tiene estructura de cuerpo. Por tanto,

a) B habrá de ser subgrupo aditivo del grupo $[C, +]$;
b) B será subgrupo multiplicativo del grupo $[C^0, \times]$.

2.732. Teorema

La condición necesaria y suficiente para que un $B \subset C$ sea subcuerpo del cuerpo $[C, +, \times]$ es que $\forall a \in B$, $\forall b \in B$,

$$[(a + (-b)) \in B] \wedge [(a \times b^{-1}) \in B].$$

Resulta superflua aquí toda demostración, que sería repetir lo dicho en Grupos (2.462) y en Anillos (2.632). Cáigase en la cuenta de que las dos condiciones establecidas son simplemente las que nos aseguran que B es subgrupo, tanto para la adición como para la multiplicación.

Que la distributividad multiplicativa sobre la adición se conserva en B, es una evidente consecuencia de los establecidos.

2.733. Característica de un cuerpo. Cuerpo primo

Aunque expuesto aquí, en Cuerpos, el concepto de característica es genérico de Anillos. Sucede que, como todo cuerpo es un anillo, el concepto alcanza su mayor generalización en la estructura de cuerpo.

Siendo $x \in C$ y $n \in Z^+$, simbolizamos (igual que en Aritmética elemental) el compuesto aditivo de n operandos iguales a x, del siguiente modo*:

$$x + x + x + \ldots (n \text{ veces} = n \cdot x);$$

pues bien: el menor $n \in Z^+$, tal que $n \cdot x = 0$, se denomina característica del cuerpo C.

Ejemplo

El cuerpo de las clases residuales, módulo 3: $[Z/3, +, \times]$, tiene de característica 3. En efecto:

$$\bar{1} + \bar{1} + \bar{1} = \bar{1} \cdot 3 = \bar{0}$$

Inmediatamente se observa que, así definida, muchos cuerpos carecen de característica; por ejemplo, el cuerpo de los racionales, en el que no existe ningún x, tal que $x \cdot n = 0$ $(n \in Z^+)$.

Se conviene en decir para estos casos que son cuerpos con característica infinita.

A este respecto, resulta interesante la siguiente

Proposición: La característica finita de un cuerpo numérico es un entero positivo primo.

Justifiquemos por reducción al absurdo. Supóngase una característica no prima $k = p \cdot q$. En ese caso,

$$k \cdot 1 = (p \cdot q) \cdot 1 = (p \cdot 1) \cdot (q \cdot 1) = 0,$$

lo que no es posible, ya que un cuerpo siempre es anillo de integridad, para lo que es exigible la ausencia de divisores del cero.

Cuerpo primo: Considérese el conjunto de todos los subcuerpos de un cuerpo $[C, +, \times]$. El más «sencillo» de todos habrá de contener el elemento unidad de C y, consecuentemente, todos sus compuestos $n \cdot 1$ (múltiplos). Ese subcuerpo, denotado C , recibe el nombre de cuerpo primo de C.

Es posible establecer un isomorfismo, muy útil por lo intuitivo, entre los cuerpos primos y los cuerpos numéricos de los racionales o de las clases residuales, módulo p, según los casos:

a) Si $[C, +, \times]$ es un cuerpo de característica infinita, el cuerpo primo C_∞ es isomorfo con el cuerpo de los racionales $[Q, +, \times]$

$$[C_\infty, +, \times] \sim [Q, +, \times].$$

b) Si $[C, +, \times]$ es un cuerpo de característica p, el cuerpo primo C_p es isomorfo con el cuerpo de las clases residuales, módulo p

$$[C_p, +, \times] \sim [Z/p, +, \times].$$

---

* Si $n \in Z^-$ ó $n \equiv 0$, los significados de la expresión $n \cdot x$ son, respectivamente, $-[(-n) \cdot x]$ y 0.

2.74. ORDENACION EN GRUPOS, ANILLOS Y CUERPOS

Hemos preferido localizar en este lugar, de un modo conjuntado, el tratamiento del orden en estas tres estructuras, en vez de abordar el tema dispersamente, en cada una de las tres ocasiones. Y ello, por los claros motivos didácticos que saltan a la vista, al leer el desarrollo que sigue.

2.741. Grupo ordenado

Sea el grupo abeliano $[G, +]$; y sea $\leq$ una relación de orden total sobre G, de modo que $[G, \leq]$ es un conjunto ordenado.

Se dice que la terna $[G, +, \leq]$ es un grupo ordenado si la estructura de grupo y la de orden son *compatibles*, en el sentido siguiente:

I. $$\forall z \in G, \quad x \leq y \Rightarrow x + z \leq y + z$$

Esta condición es equivalente a la condición

II. $$\forall a \in G, \quad \forall b \in G, \quad x \leq y \Rightarrow a + x + b \leq a + y + b$$

Demostración

A) I $\Rightarrow$ II

$$x \leq y \Rightarrow a + x \leq a + y \Rightarrow a + x + b \leq a + y + b$$

(Recuérdese que el grupo es abeliano.)

B) II $\Rightarrow$ I

$$\forall a \in G, \quad \forall b \in G, \quad x \leq y \Rightarrow a + x + b \leq a + y + b \quad (\forall b \in G);$$

en particular, si $a = 0$; $x + b \leq y + b \quad (\forall b \in G)$

si $b = 0$; $a + x \leq a + y \quad (\forall a \in G)$

Proposición 1

$$x \leq y \Leftrightarrow -y \leq -x$$

En efecto:

$$x \leq y \Rightarrow -x + x - y \leq -x + y - y \Rightarrow (-x + x) - y \leq -x + (y - y) \Rightarrow$$
$$\Rightarrow 0 - y \leq -x + 0 \Rightarrow -y \leq -x.$$

Recíprocamente, si $-y \leq -x$, por lo que acabamos de ver, será

$$-(-x) \leq -(-y), \quad \text{o sea:} \quad x \leq y.$$

2.7411. *Cono positivo de un grupo ordenado*

Se llama cono positivo de un grupo ordenado $(G, +, \leq)$ el conjunto $p^+ = \{x/x \in G, x \geq 0\}$, donde 0 es el elemento neutro del grupo.

Cada uno de los elementos del cono positivo se llama elemento *positivo*; entonces, las dos expresiones que se escriben son equivalentes:

$$x \text{ es positivo} \quad ; \quad x \geq 0.$$

Un elemento x se dice que es estrictamente positivo si $x > 0$. Un elemento x se llama *negativo* si su opuesto es positivo; o sea, las dos expresiones siguientes son equivalentes

$$x \text{ es negativo} \quad ; \quad -x \geq 0;$$

y la proposición 1 nos permite escribir equivalentemente

$$x \leq 0.$$

Si se dice que x es estrictamente negativo, se quiere indicar que $x < 0$.

Analógicamente, con el establecimiento del cono positivo, es claro que

$$p^- = \{x/ - x \in p^+\} \equiv \{x/x \leq 0\}$$

Proposición 2

$$p^+ \cap p^- = \{0\}$$

En efecto:

$$x \in p^+ \cap p^- \Rightarrow \left.\begin{matrix} x \leq 0 \\ x \geq 0 \end{matrix}\right\} \Rightarrow x = 0$$

En un grupo ordenado, la determinación del cono positivo define totalmente el orden, en virtud de la siguiente

Proposición 3

$$a \leq b \Leftrightarrow b - a \geq 0, \quad \text{o sea,} \quad b - a \in p^+$$

Si $a \leq b \Rightarrow a - a \leq b - a \Leftrightarrow b - a \geq 0$
Si $b - a \in p^+ \Rightarrow 0 \leq b - a \Rightarrow 0 + a \leq b - a + a \Leftrightarrow a \leq b$

Proposición 4

La suma de dos elementos positivos es un elemento positivo

$$a \geq 0, \quad b \geq 0 \Rightarrow a + b \geq 0$$

En efecto:

$$a \geq 0 \Rightarrow a + b \geq 0 + b = b \geq 0, \quad \text{c.q.d.}$$

Corolario: La suma de dos elementos negativos es un elemento negativo.

2.742. Anillo ordenado

Sea el anillo conmutativo $[A, +, \times]$; y sea $\leq$ una relación de orden en A, de modo que $(A, \leq)$ es un conjunto ordenado.

Se dice que la cuaterna $[A, +, \times, \leq]$ es un anillo ordenado cuando la estructura de anillo y la de orden son compatibles, en el sentido siguiente:

I. $\quad \forall z \in A \ , \ x \leq y \Rightarrow x + z \leq y + z;$

II. $\quad \forall z \in A \ , \ (x \leq y) \wedge (z \geq 0) \Rightarrow x \cdot z \leq y \cdot z$

Es claro que I asegura la naturaleza de «grupo ordenado para $[A, +, \leq]$».

La definición de cono positivo es la misma que en el caso de grupos ordenados, con las mismas propiedades a las que debemos añadir

Proposición 5

El producto de dos elementos positivos es un elemento positivo

$$(a \geq 0) \wedge (b \geq 0) \Rightarrow a \cdot b \geq 0$$

La justificación es inmediata, pues, según II,

$$(a \geq 0) \wedge (b \geq 0) \Rightarrow a \cdot b \geq 0 \cdot b = 0$$

2.7421. *Regla de los signos*

Vuélvase sobre los tres teoremas del número 2.61. Allí se habían conseguido tres resultados, sin haber establecido ningún orden en el anillo; simplemente, por la naturaleza de los elementos manejados, se llegaban a deducir las conclusiones.

Disponiendo, en este momento, del anillo ordenado, conociendo que los elementos opuestos pertenecen a distinto cono, podemos traducir a lenguaje de orden aquellos teoremas, y hablar de elementos negativos, positivos y, por supuesto, del cero.

De este modo, resulta así la regla de los signos:

a) Todo elemento del anillo ordenado por cero es cero.

b) En todo anillo ordenado, el producto de un elemento positivo por otro negativo es negativo

$$(a \geq 0) \wedge (b \leq 0) \Rightarrow a \cdot b \leq 0$$

En efecto: si $b \leq 0$, ha de ser $-b \geq 0$ y, según la proposición 5, $a \cdot (-b) \geq 0$, es decir, $a \cdot (-b) = -(a \cdot b) \geq 0$

$$a \cdot b \leq 0, \quad \text{c.q.d.}$$

c) En todo anillo ordenado, el producto de dos elementos negativos es positivo

$$(a \leq 0) \wedge (b \leq 0) \Rightarrow a \cdot b \geq 0$$

En efecto:

$$[(-a) \geq 0] \wedge [(-b) \geq 0] \Rightarrow (-a) \cdot (-b) \geq 0;$$

pero

$$(-a) \cdot (-b) = -[a \cdot (-b)] = -(-a \cdot b) = a \cdot b$$

Consecuencia de la regla de los signos es que el cuadrado de cualquier elemento (positivo o negativo) es positivo. Entonces si el anillo tiene elemento unidad 1, será:

$$1 = 1 \times 1 = 1^2 \geq 0;$$

y como $1 \neq 0$, resulta que $1 > 0$.

2.743. Cuerpo ordenado

Sea el cuerpo abeliano $[C, +, \times]$; y sea $\leq$ una relación de orden sobre C, de modo que $(C, \leq)$ es un conjunto ordenado.

Se dice que la cuaterna $[C, +, \times, \leq]$ es un cuerpo ordenado, si, considerado como anillo, es un anillo ordenado.

Así, pues, se mantiene la definición y propiedades de cono positivo.

Como un cuerpo es un anillo de integridad, es decir, no tiene divisores del cero, la regla de los signos puede expresarse así:

$$\begin{array}{ll} x > 0 & y > 0 \Rightarrow x \cdot y > 0 \\ x > 0 & y < 0 \Rightarrow x \cdot y < 0 \\ x < 0 & y > 0 \Rightarrow x \cdot y < 0 \\ x < 0 & y < 0 \Rightarrow x \cdot y > 0 \end{array}$$

Acabando el estudio del orden en estas estructuras, acumularemos a las cinco proposiciones establecidas, las dos siguientes, privativas de los cuerpos:

Proposición 6

Si $x \neq 0$, su inverso tiene el mismo signo.

Basta comprobar que $x \cdot \frac{1}{x}$ es positivo siempre, según la regla de los signos. En efecto, $x \cdot \frac{1}{x} = 1 > 0$, y esto sólo es posible si ambos factores son del mismo signo.

Proposición 7

Si $x \leq y \Rightarrow \frac{1}{y} \leq \frac{1}{x}$, siempre que $x \neq 0$ e $y \neq 0$ y con el mismo signo.

a) Si $x = y$, es claro que $1/y = 1/x$.

b) Si $x > 0$ e $y > 0 \Rightarrow x \cdot y > 0 \Rightarrow \frac{1}{x \cdot y} > 0$;

luego

$$x \leq y \Rightarrow \frac{x}{x \cdot y} \leq \frac{y}{x \cdot y} \Rightarrow \frac{1}{y} \leq \frac{1}{x}, \text{ c.q.d.}$$

c) Si $x < 0$ e $y < 0 \Rightarrow x \cdot y > 0 \Rightarrow \dfrac{1}{x \cdot y} > 0$; luego

$$x \leq y \Rightarrow \frac{x}{x \cdot y} \leq \frac{y}{x \cdot y} \Rightarrow \frac{1}{y} \leq \frac{1}{x}$$

NOTA. Si fuesen de distinto signo, la única posibilidad es que

$$x < 0 \quad \text{e} \quad y > 0 \Rightarrow x \cdot y < 0 \Rightarrow \frac{1}{x \cdot y} < 0 \Rightarrow -\frac{1}{x \cdot y} > 0,$$

luego

$$x \leq y \Rightarrow -\frac{x}{x \cdot y} \leq -\frac{y}{x \cdot y} \Rightarrow -\frac{1}{y} \leq -\frac{1}{x},$$

o lo que es igual

$$\frac{1}{x} \leq \frac{1}{y}.$$

2.744. Ordenes arquimedianos

Se entiende que un grupo aditivo ordenado goza de orden arquimediano, si establecido $0 < x < y$ es posible encontrar un natural n, tal que

$$x + x + \ldots (n \text{ veces} = n \cdot x > y)$$

Análogamente, si el grupo es multiplicativo, el concepto toma la expresión

$$1 < x < y \Rightarrow x \cdot x \ldots (n \text{ veces} = x^n > y \quad (n \in N)$$

Ejemplo 1

En $[Z, +, <]$, $0 < (+2) < (+3)$

$n \cdot (+2) > (+3)$, para todo $n \geq 2$

Ejemplo 2

En $[Q^0, \times, <]$, $1 < 4/3 < 5/2$

$(4/3)^n > 5/2$, para todo $n \geq 4$

2.75. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

2.750.

Justifíquese que en el cuerpo de los racionales se verifica siempre que

$$x^2 + y^2 > 2 \cdot x \cdot y$$

2.751.
Demuéstrese que en Q sucede siempre que $x + x^{-1} > 2$.

2.752.
Justifíquese que el orden $[Q, \geq]$ es «denso», en el sentido de que entre dos racionales cualesquiera x e y, siempre existe otro.

2.753.
En el cuerpo de las clases residuales, módulo 7, resuélvase

$$\text{I.} \qquad x + 3y = 5$$
$$\text{II.} \qquad 4x + 2y = 1,$$

en el que tanto los coeficientes como las incógnitas son clases residuales del cuerpo establecido.

2.754.
Justifíquese que el cuerpo de los racionales no tiene subcuerpos, a excepción de él mismo.

2.755.
Demuéstrese que el cuerpo ordenado de los racionales es arquimediano, probando que el grupo aditivo lo es y que el grupo multiplicativo, también.

2.756.
La llamada conjugación de complejos es una aplicación que hace corresponder a cada elemento del cuerpo C, otro cuya componente imaginaria es la opuesta de la del primero.
Demuéstrese que la conjugación es un automorfismo de C.

2.757.
Resuélvase en el cuerpo racional, la inecuación

$$x^2 + x - 1 > 0$$

2.758.
Considérese el subconjunto Q_1, de Q, formado por todos los $\frac{x}{y}$, tales que m.c.d. $(y, p) = 1$, siendo p un número primo dado.
a) Justifíquese que $[Q_1, +, \times]$ es un anillo de integridad;
b) constrúyase su cuerpo de fracciones.

2.759.
Demuéstrese que si $a \in Q$, existe un n tal que $\frac{1}{10^n} < a$.

3

ANEXOS

BIBLIOGRAFIA 3

G. CANTOR: *Contributions to the founding of the theory of transfinite numbers*. Dover Publications Inc. Nueva York.

S. S. WILKS: *Análisis estadístico elemental.*

M. JEREZ: *Probabilidad e información.*

H. CRAMER: *Elementos de la teoría de Probabilidades y algunas de sus aplicaciones*, 6.ª ed., 315 págs. Aguilar. Madrid, 1970.

S. RIOS: *Métodos estadísticos.*

VERRIEST: *Les nombres et les espaces*. Ed. Armand Colin. París.

3.1

Conjuntos numéricos

3.11. El conjunto N

3.111. *Introducción: naturales, cardinales, ordinales*

3.112. *Construcción de Peano*

3.113. *Cardinales*

3.1131. Coordinabilidad o equipotencia
3.1132. Conjuntos finitos e infinitos
3.1133. Numerabilidad. El continuo
3.1134. Números cardinales
3.1135. Orden en el conjunto de los cardinales. Teorema de Schröder-Bernstein. Teorema de Cantor
3.1136. Hipótesis del continuo

3.114. *Ordinales*

3.1141. Isomorfismo de orden
3.1142. Inducción transfinita. Secciones iniciales
3.1143. Precesión. Seguimiento. Elementos límite
3.1144. Números ordinales: ordinales finitos y transfinitos
3.1145. Orden en el conjunto ordinal

3.115. *Aritmética natural*

3.1151. Adición en N
3.1152. Multiplicación en N
3.1153. Estructura de $[\{N, 0\}, +, \times]$

3.116. *Aritmética cardinal*

3.1161. Adición de cardinales
3.1162. Multiplicación de cardinales
3.1163. Estructura de $[\mathfrak{C}, +, \times]$
3.1164. Notación potencial en el conjunto
3.1165. Los números naturales y los cardinales

3.117. *Aritmética ordinal*

3.1171. Adición ordinal
3.1172. Multiplicación ordinal

3.12. El conjunto Z

3.121. *Necesidad de ampliar N*

3.122. *Simetrización del semigrupo abeliano cancelativo* $[\{N, 0\}, +]$

3.1221. Condiciones de simetrización
3.1222. Relación de equivalencia sobre N^2, agente de clasificación
3.1223. Representantes canónicos. Enteros positivos, negativos y nulo
3.1224. Adición inducida en Z

3.123. *El grupo aditivo de los enteros relativos Z*

3.124. *El semigrupo* $[N, +]$ *sumergido en el grupo* $[Z, +]$

3.125. *Orden en* $[Z, +]$

3.126. *La multiplicación en* Z

3.127. *El anillo multiplicativo de los enteros relativos*

3.128. *El anillo ordenado* $[Z, +, \times]$

3.129. *Divisibilidad en* Z

3.1291. Relación de divisibilidad
3.1292. División euclídea
3.1293. Relación de congruencia, módulo m
3.1294. Divisibilidad e ideales en Z

3.13. El conjunto Q

3.131. *Necesidad de ampliar* Z

3.132. *Creación del cuerpo* $[Q, +, \times]$. *Simetrización del dominio de integridad* $[Z, +, \times]$

3.1321. El semigrupo a simetrizar $[Z, \times]$
3.1322. El cuerpo de fracciones del dominio de integridad Z

3.133. *El dominio de integridad* Z *sumergido en el cuerpo* Q

3.134. *El cuerpo ordenado* $[Q, +, \times, \leq]$

3.14. Aplicabilidad. Automatismos y destrezas

3.1

Conjuntos numéricos

3.11. EL CONJUNTO *N*

3.111. Introducción: naturales, cardinales, ordinales

El tema del número natural, en la base de la Aritmética, desde las más remotas horas del hombre inteligente, es, sin embargo, una parcela sumamente difícil de la Matemática.

Rozando la profunda filosofía del saber, la numerabilidad y lo transfinito, el continuo y los ordinales-límite, así como tantas otras cuestiones, abiertas todavía hoy a la investigación, presentan la extrema dificultad de lo esencialmente simple.

Continuamente, al borde de la paradoja —y cayendo en ella— a la luz relámpago que produce la proximidad de las cosas realmente simples, la vereda transcurre sobre el precipicio de la contradicción y bajo las cumbres de las esencias; y todo —quede dicho sin rubor— apenas es algo más que lo que hacía el pastor ancestral cuando, a la tarde, contaba con guijarros sus rebecos.

Se trata, pues, de un tema difícil, cuyo desarrollo a nivel de iniciación (¡intentar la simplificación de lo simple!) es tarea de éxito dudoso. Por eso mismo, en estos niveles a que nos referimos, es notable el confusionismo: puede que con frecuencia el buen propósito de una exposición didáctica elemental haya provocado entender que los naturales son cardinales u ordinales, según el ángulo de su contemplación; entendemos que es un error gratuito que a nada conduce y al que se le puede aplicar la estupenda frase de Ampère: «los errores tienen vida tenaz; cuando el tiempo no los destruye, los embalsama».

En la línea que se dice, optamos por presentar primero la construcción axiomática de Peano para los naturales.

3.112. Construcción de Peano

Se admite la existencia de un conjunto no vacío, denotado N y llamado conjunto de los números naturales, determinado por los siguientes axiomas:

A_1) Existe un elemento, llamado *uno* y denotado 1

$$1 \in N$$

A_2) Para cada natural, existe otro, único, llamado «siguiente»

$$\forall a \in N,\ \exists^* a^+ / a^+ \in N$$

A_3) Todo natural siguiente es distinto de 1

$$a^+ \neq 1$$

A_4) Si dos naturales siguientes son iguales, los naturales de los que lo son, también son iguales

$$a^+ \in N,\ b^+ \in N,\ a^+ = b^+ \Rightarrow a = b$$

A_5) *Principio de inducción**: Siendo S un subconjunto de N al que pertenece el 1, si el hecho de que el natural a pertenezca a S implica que su siguiente a^+ también es de S, entonces resulta que $S \equiv N$. Es decir:

$$\forall S \subset N,\ [(1 \in S) \wedge (a \in S \Rightarrow a^+ \in S)] \Rightarrow S \equiv N$$

La axiomática precedente permite establecer el conjunto de los números naturales N. En efecto:

1) existe un elemento «inicial», siguiente de ninguno: el 1;
2) el uno tiene un siguiente (A_2), distinto de él (A_3), único (A_4): es el denotado 2 y llamado «dos»;
3) de igual modo, y con las mismas bases axiomáticas, se generan el 3, 4, 5, 6, ...

Queda establecido así el conjunto de los números naturales

$$N = \{1, 2, 3, 4, \ldots\}$$

La axiomática establecida implica para el conjunto N una buena ordenación y, por consiguiente, una ordenación total. En efecto:

Todo $a \in N$ descompone al conjunto de los naturales en tres subconjuntos

$$A = \{1, 2, 3, \ldots, a^-\}, \quad \{a\} \quad \text{y} \quad A' = \{a^+, (a^+)^+, \ldots\},$$

* Este axioma de Peano no es más que la particularización para N de un principio más amplio, válido y demostrable para todo conjunto bien ordenado, como es el caso de N.

denominándose *sección inicial de a* el conjunto A de todos los naturales estrictamente anteriores a a.

Se establece la siguiente relación:

$$a, b \in N,\ (b \leq a) \Leftrightarrow (b \in A) \vee (b \in \{a\})$$

La relación establecida es de orden, ya que es

a) *reflexiva*:

$$\forall a \in N,\ a \in \{a\} \Rightarrow a \leq a$$

b) *antisimétrica*:

$$a, b \in N, \begin{Bmatrix} b \leq a \Rightarrow (b \in A) \vee (b \in \{a\}) \\ a \leq b \Rightarrow (a \in B) \vee (a \in \{b\}) \end{Bmatrix} \Rightarrow$$

$$\Rightarrow [(b \in A) \vee (b \in \{a\})] \wedge [(a \in B) \vee (a \in \{b\})] \equiv$$
$$\equiv [(b \in A) \wedge ((a \in B) \vee (a \in \{b\}))] \vee [(b \in \{a\}) \wedge ((a \in B) \vee (a \in \{b\}))] \equiv$$
$$\equiv [(b \in A) \wedge (a \in B)] \vee [(b \in A) \wedge (a \in \{b\})] \vee [(b \in \{a\}) \wedge (a \in B)] \vee$$
$$\vee [(b \in \{a\}) \wedge (a \in \{b\})] \equiv$$
$$\equiv \phi \vee \phi \vee \phi \vee [(b \in \{a\}) \wedge (a \in \{b\})] \equiv$$
$$\equiv [(b \in \{a\}) \wedge (a \in \{b\})] \Rightarrow a \equiv b$$

c) *transitiva*:

$$a, b, c \in N \quad \begin{matrix} a \leq b \\ b \leq c \end{matrix} \Rightarrow a \leq c$$

La justificación no presenta dificultad alguna;

Además:

d) $\forall A \subset N$ tiene primer elemento, según se desprende de los axiomas A_1, A_2 y A_3; y

e) $\forall a \in N, \forall b \in N\ (a \leq b) \vee (b \leq a)$.

Efectivamente, $\{a, b\} \subset N$ tiene primer elemento por ser $[N, \leq]$ buena ordenación; luego en cada subconjunto binario de N, el que es primer elemento es anterior al otro; en fin: ambos son siempre comparables.

3.113. Cardinales

3.1131. *Coordinabilidad o equipotencia*

Sean los conjuntos A y B. Si es posible establecer una biyección entre sus elementos, se dirá que A y B son conjuntos coordinables o equipotentes, y se denotará $A \sim B$. Simbólicamente se define:

$$A \sim B \Leftrightarrow f\colon A \to B \text{ biyección}$$

Resulta primario e intuitivo comprender que si se trata de conjuntos finitos, son equipotentes aquellos que «tengan el mismo número de elementos». Y en esa línea de intuición poco analítica, cabría pensar que, a su vez, todos los conjuntos infinitos son biyeccionables y, por tanto, equipotentes. De hecho, tal error se mantuvo hasta que Georg Cantor definiera la equipotencia como anteriormente ha quedado establecida. No todos los conjuntos infinitos son equipotentes entre sí.

La relación de equipotencia es una relación de equivalencia sobre el conjunto de los conjuntos. En efecto: resulta inmediato que es

1) *reflexiva*: $\forall A \in C, \quad A \sim A$
2) *simétrica*: $A, B \in C, \quad A \sim B \Rightarrow B \sim A$
3) *transitiva*: $A, B, D \in C, \quad (A \sim B) \wedge (B \sim D) \Rightarrow A \sim D$

Esta naturaleza de la relación de equipotencia la capacita para ser instrumento de clasificación y partición sobre los conjuntos, lo que permitirá después crear el conjunto de los números cardinales.

3.1132. *Conjuntos finitos e infinitos*

Conviene matematizar estos dos conceptos, a los que nos hemos venido refiriendo con manifiesta gratuidad, en sus acepciones vulgares, suficientemente peligrosas para inducir a error.

Conjunto infinito: A es un conjunto infinito si es equipotente con una de sus partes.

Ejemplo 1

Sean los conjuntos N y $N \supset P = \{x/(x \in N) \wedge (x = \dot{3})\}$ y la función $f: N \to P$, de criterio $f(x) = 3x$.

La aplicación f resulta ser inyectiva y sobreyectiva, es decir, se trata de una biyección.

Así, pues, los conjuntos N y P son equipotentes: N es un conjunto infinito

$$N \sim P$$

Ejemplo 2

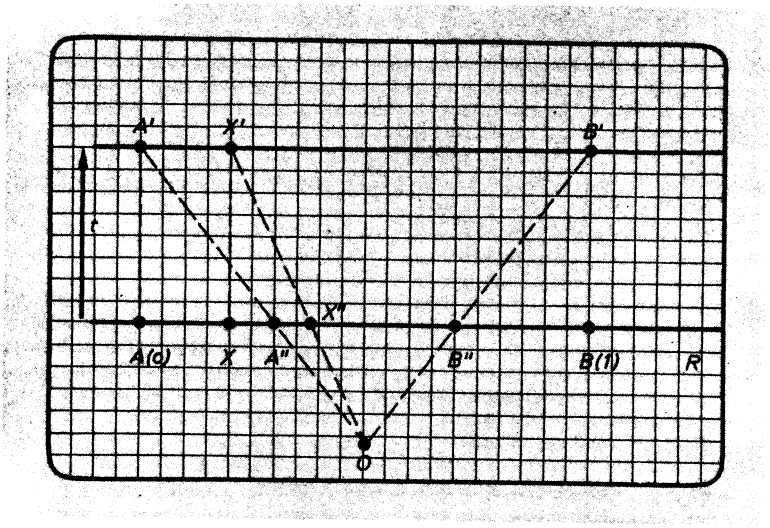
. Sea el cerrado real [0, 1] representado por todos los puntos del segmento $\overline{AB}$ de la recta real R.

Y sea otro cerrado real [0, 3; 0, 7], representado en el segmento real $\overline{A''B''}$.

Considérese la función $f: \overline{AB} \to \overline{A''B''}$, tal que haga corresponder a cada $x \in [0, 1]$ un $f(x) \in [0, 3; 0, 7]$, obtenido trasladando primero a x, según t, y proyectando luego $t(X) = X'$, desde un punto fijo 0, sobre R, en X''; de modo que $f(X) = X''$. Esta aplicación f es claramente inyectiva y sobreyectiva; se trata, pues, de una biyección.

Se ha conseguido una aplicación biyectiva entre el cerrado real [0, 1] y un subconjunto suyo [0, 3; 0, 7], lo que permite escribir

$$[0, 1] \sim [0, 3; 0, 7]$$



La equipotencia establecida exige que el conjunto [0, 1] sea infinito.

Conjunto finito es aquel que no es equipotente con alguna de sus partes. Todo conjunto finito presenta las siguientes notas esenciales:

a) es posible su ordenación con primero y último elementos;
b) todo subconjunto ordenado también tiene primero y último elementos.

3.1133. *Numerabilidad. El continuo*

Si un conjunto A es equipotente con el conjunto de los números naturales N, se dice que es *numerable* y se le asigna el propio cardinal de N, representado por $\aleph_0$ (primera letra del alfabeto hebreo; léase «alef cero»).

Por extensión, todo conjunto finito se considera numerable por ser coordinable con un subconjunto de N.

Ejemplo 1

Cualquier sucesión infinita de elementos distintos es un conjunto numerable. En efecto: una sucesión es una función cuyo dominio de la variable es N. Si sus términos son distintos, $f(N) = S_N$ es inyectiva y sobreyectiva, de modo que

$$S_N \sim N$$

Se enuncian a continuación algunos teoremas interesantes, referibles a la numerabilidad.

TEOREMA 1. Todo conjunto infinito tiene, al menos, un subconjunto numerable.

TEOREMA 2. Todo subconjunto de un conjunto numerable es numerable.

Teorema 3. La unión de todos los conjuntos disjuntos numerables de una familia numerable es numerable.

Teorema 4. El conjunto de los números racionales Q es numerable.

En efecto: Sea $Q = Q^+ \cup \{0\} \cup Q^-$.
Establezcamos la función f: $Q^+ \to N \times N$, con el siguiente criterio:

$$\begin{array}{l} Q^+ \xrightarrow{f} N \times N \\ a/b \longrightarrow f(a/b) = (a, b) \end{array}$$

Es claro que se trata de una inyección y Q^+ será coordinable o equipotente con un subconjunto de $N \times N$.

$$Q^+ \sim A \subset (N \times N).$$

Admitido que $N \times N$ es numerable (lo que, por otra parte, es inmediato de probar) y según el teorema 2, el conjunto Q^+ es numerable.

De idéntico modo se procedería con Q^-; así es que, según el teorema 3, se concluye: el conjunto de los racionales Q es numerable.

Existen conjuntos infinitos con los que no es posible establecer una biyección con los naturales; no son equipotentes a N y se dice que son conjuntos no numerables.

El conjunto infinito no numerable de mayor representatividad es el cerrado real $[0, 1]$, el intervalo unidad.

Demostremos que, en efecto, el intervalo $[0, 1]$ no es numerable. Se construye una demostración al absurdo:

1. Admítase que $A = [0, 1]$ es numerable, lo que supondría que el intervalo se podría expresar como una sucesión (véase ejemplo 1).

$$A = \{\alpha_1, \alpha_2, \ldots, \alpha_n \ldots\}, \quad n \in N$$

2. Es posible escribir cada término de la sucesión en forma decimal con un número ilimitado de cifras*. Así:

$$\begin{array}{l} \alpha_1 = 0, a_{11}a_{12} \ldots a_{1n} \ldots \\ \alpha_2 = 0, a_{21}a_{22} \ldots a_{2n} \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_n = 0, a_{n1}a_{n2} \ldots a_{nn} \ldots \end{array}$$

3. Sea ahora el real $\beta \in A$

$$\beta = 0, b_1b_2 \ldots b_n \ldots,$$

---

* Utilícense los miembros convenientes de estas igualdades correctas:

0,1000... = 0,0999...; 0,0300... = 0,02999...; 1,00... = 0,999...; etc.

construido de manera que ninguna de sus cifras decimales sea nula ni coincidente con la del mismo orden, en cada uno de los términos de la sucesión planteada, es decir:

$$(b_n \neq 0) \wedge (b_n \neq a_{nn})$$

4. De este modo se consigue un $\beta \neq a_n$, $\forall n \in N$; o lo que es igual,

$$\beta \notin A,$$

en contra de lo establecido; luego

$A = [0, 1]$ no es numerable, c.q.d.

De todo conjunto infinito no numerable, equipotente con el intervalo unidad $[0, 1]$, se dice que tiene la *potencia del continuo* y se le asigna el propio cardinal de $[0, 1]$, denotado $\aleph_1$ (alef uno).

Ejemplo 2

Sea el cerrado $[0, \pi]$ y la función

$$\begin{array}{c} [0, 1] \xrightarrow{f} [0, \pi] \\ x \longrightarrow f(x) = \pi \cdot x \end{array}$$

Siendo claramente f inyectiva y exhaustiva, se establece la equipotencia de ambos intervalos, resultando el cardinal de $[0, \pi]$, $\aleph_1$.

Ejemplo 3

Se establece la función

$$\begin{array}{c} [0, \pi] \xrightarrow{\text{ctg}} R \\ x \longrightarrow \text{ctg } x \end{array}$$

Es evidente que, siendo inyectiva y exhaustiva,

$$R \sim [0, \pi].$$

El conjunto de los reales tiene la potencia del continuo y su cardinal es $\aleph_1$.

3.1134. *Números cardinales*

Al final del número 3.1131 quedó establecida la naturaleza de la relación de equipotencia o coordinabilidad como una relación de equivalencia y, por tanto, con capacidad de clasificar y partir todos los conjuntos* en clases disjuntas, cada una de las cuales es un *número cardinal.*

---

* El conjunto de todos los conjuntos es un concepto paradójico. Si $\mathcal{C}$ es el conjunto de *todos* los conjuntos, ha de contener como subconjunto, al conjunto potencia $2^{\mathcal{C}}$:

$$2^{\mathcal{C}} \subset \mathcal{C} \Rightarrow \text{card}(2^{\mathcal{C}}) \leq \text{card}(\mathcal{C}).$$

Según el teorema de Cantor, ha de suceder que $\text{card}(2^{\mathcal{C}}) > \text{card}(\mathcal{C})$. He ahí la contradicción. Es evidente que esta nota ha de leerse de nuevo, tras el estudio del teorema de Cantor.

Los cardinales pueden ser finitos o infinitos. Los primeros son el cardinal de la familia de conjuntos equipotentes con el ϕ y los de todas las familias de equipotencia de cada uno de los subconjuntos propios de N:

$$\left.\begin{array}{r} \operatorname{card}(\phi) = 0 \\ \operatorname{card}(\{1\}) = 1 \\ \operatorname{card}(\{1, 2\}) = 2 \\ \operatorname{card}(\{1, 2, 3\}) = 3 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{array}\right\} \text{cardinales finitos;}$$

de los segundos, de número ilimitado (a justificar luego, por el teorema de Cantor), se han establecido hasta ahora dos:

$$\left.\begin{array}{r} \operatorname{card}(N) = \aleph_0 \\ \operatorname{card}([0, 1]) = \aleph_1 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{array}\right\} \text{cardinales infinitos}$$

3.1135. *Orden en el conjunto de los cardinales. Teorema de Schröder-Bernstein. Teorema de Cantor*

Sean A y B dos conjuntos, tales que $\operatorname{card}(A) = a$ y $\operatorname{card}(B) = b$.

1.° Se establece una relación entre los conjuntos A y B, con el siguiente criterio y notación:

$$A \lessapprox B \Leftrightarrow \exists f: A \to B \text{ inyectiva.}$$

Se dirá entonces que «A precede a B».

2.° Asociada a la relación establecida, aparece otra entre sus cardinales

$$A \lessapprox B \Leftrightarrow a \leq b$$

3.° Ambas relaciones son reflexivas, antisimétricas y transitivas.

Reflexividad

$$A \lessapprox A \Rightarrow a \leq a$$

puesto que la función idéntica siempre es inyectiva:

$$A \xrightarrow{I} A$$

Antisimetría (Teorema de Schröder-Bernstein)

$$(A \lessapprox B) \wedge (B \lessapprox A) \Rightarrow A \sim B \Rightarrow (a \leq b) \wedge (b \leq a) \Rightarrow a \equiv b$$

Transitividad

$$\left.\begin{array}{l} A \lessapprox B \\ B \lessapprox C \end{array}\right\} \Rightarrow A \lessapprox C \qquad \left.\begin{array}{l} a \leq b \\ b \leq c \end{array}\right\} \Rightarrow a \leq c$$

ya que el producto de dos funciones inyectivas siempre es una inyección.

Se ha establecido con ello un orden en el conjunto de los cardinales.

Por lo que se refiere a la relación de orden en los cardinales finitos, adviértase que se trata de una simple extensión de la relación de orden establecida en N; de modo que

$$\underset{\text{cardinales}}{a \leq b} \Leftrightarrow \underset{\text{naturales}}{a \leq b}$$

Respecto a los cardinales infinitos, analicemos el orden en los dos vistos hasta ahora:

Se puede establecer una inyección de N en R, asignando a cada natural el real isomórfico con él (en lenguaje más próximo pero incorrecto se diría: N es un subconjunto de R); por tanto,

$$N \xrightarrow[\text{inyec.}]{f} R \Leftrightarrow N \lesssim R \Leftrightarrow \text{card}(N) \leq \text{card}(R).$$

$$\aleph_0 \leq \aleph_1$$

Y teniendo en cuenta que R no es enumerable, es decir, que $\aleph_0 \neq \aleph_1$, la relación de orden establecida se puede restringir a una de orden estricto

$$\aleph_0 < \aleph_1$$

TEOREMA *de Cantor*

Establecido un cardinal cualquiera, siempre existe otro mayor que él.

En efecto: entre un conjunto cualquiera A y el conjunto de sus partes $P(A)$, siempre se verifica que

$$A \lesssim P(A)$$

Siendo $a = \text{card}(A)$, sucede que

$$A \lesssim P(A) \Leftrightarrow a < 2^a,$$

lo que justifica el teorema.

Finalmente, apuntemos que el orden establecido en el conjunto de los cardinales es un orden total (ley de tricotomía). Se quiere decir que

$$\forall a, b \in \mathfrak{C},\ (a < b) \vee (a = b) \vee (a > b).$$

Esta ley es consecuencia inmediata del teorema de la buena ordenación.

3.1136. *Hipótesis del continuo*

Según el teorema de Cantor aplicado al cardinal de los numerables,

$$\aleph_0 < 2^{\aleph_0}$$

También quedó establecido anteriormente que la potencia del continuo es estrictamente superior al cardinal de los numerables

$$\aleph_0 < \aleph_1$$

Se puede demostrar que la relación entre ambos cardinales es

$$2^{\aleph_0} = \aleph_1$$

Tras este resultado es inmediata la pregunta: ¿existirá algún cardinal superior al cardinal numerable e inferior a la potencia del continuo?; o lo que es igual: ¿hay un cardinal α, tal que

$$\aleph_0 < \alpha < \aleph_1?$$

La hipótesis del continuo contesta negativamente, a saber:

> *Hipótesis del continuo*: No existe un cardinal α, tal que $\aleph_0 < \alpha < \aleph_1$.

Un enunciado equivalente al anterior, que describe los términos próximos de la investigación al respecto es

> *Hipótesis del continuo*: Toda parte infinita de R es equipotente a N o a R.

La «andadura matemática» respecto a la hipótesis del continuo es sumamente sugestiva, a la par que nada lejana.

Hacia 1930 los lógicos, encabezados por K. Gödel, consiguieron demostrar la imposibilidad de justificar el hecho de que toda proposición ha de ser verdadera o falsa; es decir, que podrían existir proposiciones «indecidibles», lo cual arruinaría la restrictividad de la axiomática matemática que, de este modo, permitiría la aparición de proposiciones lógicamente ambiguas (!).

Desde los primeros años del siglo XX hasta Gödel, y después de él, se ha intentado establecer al margen de toda ambigüedad lógica, la hipótesis del continuo, sin éxito alguno. Así fueron las cosas, hasta que en 1963, el joven matemático americano Paul Cohen, ante la sorpresa de muchos y el asombro de todos, corroborando las ideas de Gödel, alcanzó la extraordinaria justificación de que la hipótesis del continuo es una proposición «indecidible»; o lo que es igual: que la hipótesis del continuo es un axioma *independiente* dentro del edificio matemático establecido y que, aceptada o negada, sustenta dos matemáticas correctas y diferentes.

3.114. Ordinales

3.1141. *Isomorfismo de orden*

Sean dos conjuntos ordenados $[A, \lhd]$ y $[B, \lhd]$ y una biyección f entre ellos, tal que

$$\forall a_1 \in A,\ \forall a_2 \in A,\ (a_1 \lhd a_2) \Leftrightarrow (f(a_1) \lhd f(a_2)).$$

Se dice entonces que $f: [A, \curlywedge] \to [B, \curlywedge]$ es un isomorfismo de orden, y escribimos para los conjuntos

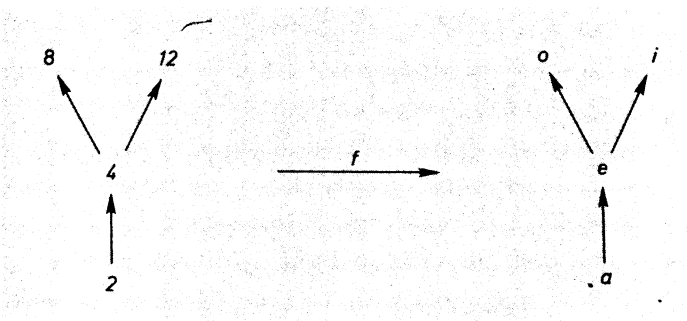
$$A \backsim B.$$

Ejemplo

Sea el conjunto $A = \{2, 4, 8, 12\}$ ordenado mediante la relación de divisibilidad x/y. Considérese también el conjunto de vocales $V = \{a, e, o, i\}$ ordenado mediante la secuencia lexicográfica de la bivariante semántica que se expresa:

$$\text{male} \lessdot \begin{matrix} \text{cón} \\ \text{tín} \end{matrix}$$

Los diagramas de orden que se establecen denuncian claramente la posibilidad de una biyección entre ambos conjuntos, que conserve el orden:



$$f = \{(2, a),\ (4, e),\ (8, o),\ (12, i)\}$$

Consecuencias inmediatas del isomorfismo de orden, son las proposiciones

Primera. Si $[A, \curlywedge]$ es un orden total y existe el isomorfismo $[A, \curlywedge] \xrightarrow{f} [B, \curlywedge]$, el conjunto B está totalmente ordenado.

Segunda. Los elementos notables en un isomorfismo de orden se corresponden (primeros y últimos elementos, maximales y minimales).

Tercera. Si $[A, \curlywedge] \xrightarrow{f} [B, \curlywedge]$ es un isomorfismo de orden, los conjuntos A y B son equipotentes:

$$A \backsim B \Rightarrow A \sim B$$

Cuarta. Todos los conjuntos finitos equipotentes, totalmente ordenados, presentan buena ordenación y son equipotentes entre sí.

El establecimiento de los números ordinales descansa directamente sobre la siguiente

Quinta. El isomorfismo de orden es una relación de equivalencia. En efecto, posee

Reflexividad: $A \sim A, \ \forall A$

Simetría: $A \sim B \Leftrightarrow B \sim A$

Transitividad: $\left.\begin{matrix} A \sim B \\ B \sim C \end{matrix}\right\} \Rightarrow A \sim C$

3.1142. *Inducción transfinita. Secciones iniciales*

Sea un conjunto A bien ordenado y a un elemento de él. Se denomina sección inicial de a, denotada $s(a)$, al conjunto de todos los elementos de A, estrictamente anteriores a a, de modo que

$$\forall x \in s(a), \ x \lhd a$$

Con la anterior noticia, se establece el principio de inducción transfinita que dicta: Siendo $[A, \lhd]$ una buena ordenación y, siendo a_0 el primer elemento de ella

$$[(a_0 \in B) \wedge ((s(a) \subset B) \Rightarrow a \in B)] \Rightarrow B \equiv A,$$

que se lee:

Si un subconjunto de un conjunto bien ordenado contiene al primer elemento del orden y el hecho de que incluya a la sección inicial de un elemento, implica que contiene al elemento, entonces ese subconjunto coincide con el conjunto total.

Dejemos apuntadas a continuación unas proposiciones que no demostramos, pero que van a resultar muy útiles en la construcción que pretendemos.

Sexta. Si dos conjuntos bien ordenados están ligados mediante un isomorfismo de orden, éste es único.

Séptima. Si dos conjuntos A y B están bien ordenados, o son isomorfos o uno de ellos lo es con una sección inicial del otro.

Octava. Un conjunto bien ordenado no puede ser isomorfo con alguna de sus secciones iniciales*

3.1143. *Precesión. Seguimiento. Elementos límite*

Sea el orden $[A, \lhd]$ y los elementos $a \in A$ y $b \in A$. Si sucede que no existe ningún $c \in A$, tal que

$$a \lhd c \lhd b,$$

entonces se dice que

a es precedente de b

y que

b es siguiente de a

---

* Cuando quede establecido el conjunto de *todos* los ordinales, se dará cuenta de la famosa paradoja de Burali-Forti, en abierta contradicción con esta proposición 8.ª.

Ejemplo 1

En el orden racional $[Q, <]$ ningún elemento precede ni sigue a algún otro. En efecto: dados dos cualesquiera racionales $x < y$, siempre es posible encontrar otro z, tal que

$$x < z < y$$

Basta, por ejemplo, hacer $z = \frac{x + y}{2}$.

Novena. Cualquier elemento de una buena ordenación tiene siguiente, a excepción del posible último elemento.

Contra lo que podría parecer, no existe una proposición paralela a la novena, referible a la precesión. Es posible encontrar dentro de una buena ordenación elementos distintos del primero, que no tienen precedente. A tales elementos se les denomina *elementos límite.*

Ejemplo 2

Sean los conjuntos $A = \{1;\ 1{,}3;\ 1{,}33;\ \ldots\}$ y $B = \{1{,}4;\ 1{,}44;\ 1{,}444;\ \ldots\}$ y los órdenes

$$[A, <] \quad \text{y} \quad [B, <]$$

La reunión de los órdenes propuestos produce el conjunto ordenado

$$\{1;\ 1{,}3;\ 1{,}33;\ 1{,}333;\ \ldots;\ 1{,}4;\ 1{,}44;\ 1{,}444;\ \ldots\}$$

En él su elemento 1 no tiene precedente por ser primer elemento; pero el elemento 1,4 no lo es y tampoco tiene precedente: se trata de un elemento-límite.

3.1144. *Números ordinales: ordinales finitos y transfinitos*

A) *Tipos ordinales*

La quinta proposición del número 3.1141 establecía que el isomorfismo de orden es una relación de equivalencia y, como tal, clasifica y parte en clases disjuntas al conjunto de los conjuntos ordenados.

Sea A un conjunto totalmente ordenado y $\mathfrak{A}$ la familia de conjuntos isomorfos con él. $\mathfrak{A}$ recibe el nombre de «tipo ordinal de A».

El tipo ordinal al que pertenece N se signa con la letra ω; y la familia de orden al que pertenecen los enteros se suele representar con la letra π.

Ejemplo 1

El conjunto $A = \{x/x$ es natural impar$\}$, ordenado con la relación $<$, tiene como tipo ordinal ω, pues

$$[A, <] \xrightarrow{f} [N, <] \text{ es un isomorfismo.}$$

Ejemplo 2

Si se decide representar con un apóstrofe (') el tipo ordinal correspondiente al conjunto ordenado con la relación inversa, no siempre se mantiene el isomorfismo de orden. Tal sucede con el ejemplo 1, de modo que $\omega \neq \omega'$.

Pero sí es isomorfismo, por ejemplo,

$$[Z, <] \overset{f}{\rightarrow} [Z, >],$$

lo que permite escribir en este caso

$$\pi = \pi'$$

B) *Número ordinal* es el tipo ordinal de un conjunto bien ordenado.

Como puede observarse, el isomorfismo de orden, que es relación de equivalencia, actuando sobre los conjuntos bien ordenados produce sus tipos de orden que, en este caso, reciben el nombre de números ordinales.

Si se llama λ a la familia de conjuntos bien ordenados a la que pertenece el conjunto A, se escribirá:

$$\lambda = \text{ord}(A).$$

Los números ordinales pueden ser finitos y transfinitos. Los números ordinales finitos son los que corresponden a las familias a las que pertenecen los conjuntos bien ordenados que se tabulan:

$$\begin{array}{rcr} \phi & ; & \text{ord}(\phi) = 0 \\ \{1\} & ; & \text{ord}(\{1\}) = 1 \\ \{1, 2\} & ; & \text{ord}(\{1, 2\}) = 2 \\ \{1, 2, 3\} & ; & \text{ord}(\{1, 2, 3\}) = 3 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \end{array}$$

Anteriormente quedó apuntado que el conjunto de los números naturales pertenece al ordinal representado ω.

$$\omega = \text{ord}(N)$$

3.1145. *Orden en el conjunto ordinal*

Sean A y B dos conjuntos del conjunto de las buenas ordenaciones y sean sus ordinales λ y μ, de modo que

$$\lambda = \text{ord}(A) \quad ; \quad \mu = \text{ord}(B)$$

En el conjunto de los ordinales a los que pertenecen λ y μ, se establece la siguiente relación

$$\lambda < \mu \Leftrightarrow A \sim s(b), \; b \in B$$

La relación es antisimétrica y transitiva; y la relación

$$\lambda \leq \mu \Leftrightarrow [(A \sim s(b),\ b \in B) \vee (A \sim B)]$$

es un orden amplio total sobre el conjunto de ordinales al que pertenecen λ y μ.

Puede justificarse por la proposición

Décima. Todo conjunto de ordinales resulta ser una buena ordenación con la relación $\lambda \leq \mu$.

Considérese ahora un ordinal μ y establézcase su sección inicial $s(\mu)$, de modo que $\forall \lambda \in s(\mu),\ \lambda < \mu$.

La décima proposición exige que $s(\mu)$ sea un conjunto bien ordenado lo que, a su vez, implica que ord$(s(\mu))$ existe.

Se demuestra que

Undécima. Todo número ordinal coincide con el ordinal de su sección inicial

$$\mu = \text{ord}(s(\mu)).$$

O dicho de un modo simplista: un número ordinal es el conjunto de todos los ordinales que le preceden.

Esta proposición es extraordinariamente importante, pues permite construir el conjunto de los ordinales, a resguardo de la paradoja de Burali-Forti, a la que se avoca irremediablemente, de intentar otra construcción.

La paradoja apuntada consiste en lo siguiente:

a) Sea $\mathfrak{O}$ el conjunto de todos los números ordinales.
b) Según la décima proposición, $[\mathfrak{O}, \leq]$ es buena ordenación; sea $\delta = \text{ord}(\mathfrak{O})$.
c) Considérese ahora la sección inicial $s(\delta)$ de todos los $a \in \mathfrak{O} / a < \delta$.
d) Pero, según la undécima proposición,

$$\delta = \text{ord}(s(\delta));$$

e) resulta, entonces, que

$$\text{ord}(\mathfrak{O}) = \text{ord}(s(\delta)),$$

en abierta contradicción con la octava proposición, que dice que un conjunto nunca es isomorfo con alguna de sus secciones iniciales.

Así, pues, basándonos en la undécima proposición, se construye el conjunto ordinal de la siguiente manera:

$$\left.\begin{array}{l} 0 \equiv \phi \\ 1 \equiv \{0\} \\ 2 \equiv \{0, 1\} \\ 3 \equiv \{0, 1, 2\} \\ \vdots \quad\quad \vdots \\ \vdots \quad\quad \vdots \end{array}\right\} \text{ ordinales finitos}$$

$\omega \equiv \{0, 1, 2, 3, 4, \ldots\}$: 1.er ordinal-límite
$\omega + 1 \equiv \{0, 1, 2, 3, \ldots \omega\}$
$\omega + 2 \equiv \{0, 1, 2, \ldots \omega, \omega+1\}$
. . . . . .
. . . . . .
$\omega_2 \equiv \{0, 1, 2, \ldots \omega, \omega+1, \omega+2, \ldots\}$: 2.° ordinal-límite
$\omega_2 + 1 \equiv \{0, 1, 2, \ldots \omega, \omega+1, \omega+2, \ldots \omega_2\}$
. . . . . .
. . . . . .
$\omega_3 \equiv \{0, 1, 2, \ldots \omega, \omega+1, \omega+2, \ldots \omega_2, \omega_2+1, \ldots\}$:
. . . . . 3.er ordinal-límite
. . . . . .
$\omega^2 \equiv \{\ldots/\ldots/\ldots \omega_\omega\}$: ω-ésimo ordinal-límite
. . . . . .
. . . . . .
$\omega^3 \equiv \{\ldots/\ldots/\ldots///\ldots \omega_\omega^2\}$: ordinal-límite
. . . . . .
. . . . . .
$\omega^\omega = \{.. \quad .. \quad .. \quad .. \quad ..\}$: ordinal-límite
. . . . . .
. . . . . .
$(\omega^\omega)^\omega = \{.. \quad .. \quad .. \quad .. \quad ..\}$: ordinal-límite
. . . . . .
. . . . . .
$((\omega^\omega)^\omega)^\omega = \{.. \quad .. \quad .. \quad .. \quad ..\}$: ordinal-límite
. . . . . .
. . . . . .

ordinales transfinitos

3.115. Aritmética natural

Establecido el conjunto N y en él una relación de orden, ahora procede su estructuración algebraica, definiendo las operaciones internas que van a dotar de estructura de semianillo abeliano con elemento unidad* al conjunto $N \cup \{0\}$.

3.1151. *Adición en N*

$$\forall (a, b) \in N \times N, \ \exists^* c \in N / a + b = c, \qquad [1]$$

según los siguientes axiomas de definición:

I. $Aa \in N, \ a + 1 = n^+$.
II. $a \in N, \ b \in N, \ a + b^+ = (a + b)^+$, si $a + b$ existe.

---

* Adosar a N el cero en este momento no es, como pudiera parecer, un inevitable «remiendo». Hemos preferido hacerlo así, en lugar de haber establecido su existencia en N, mediante un axioma previo. Diremos simplemente, que «cero» es el natural x que verifica la igualdad en N,

$$a + x = x + a = a$$

De todos modos, siempre que convenga, explicitaremos su consideración, denotando el conjunto que lo contiene, así: $\{N, 0\}$.

La expresión [1] indica que la adición así definida es una ley de composición interna u operación, cosa que ha de probarse a partir de los dos axiomas de definición. Para ello, se parte del quinto axioma de Peano o principio de inducción:

a) Sea $B \subset N$ un subconjunto cuyos elementos b verifican que

$$\forall a \in N,\ a + b \in N;$$

en particular, como $a + 1 = a^+ \in N \Rightarrow 1 \in B$

b) Según II,

$$a + b^+ = (a + b)^+ \in N,$$

lo que exige que $b^+ \in B$; luego $B \equiv N$

Queda demostrado así que el resultado c de sumar dos naturales a y b es único y pertenece al conjunto de los naturales. La adición en N obedece a las siguientes leyes:

1. *Asociatividad*

$$\forall a,\ b,\ c \in N,\ a + (b + c) = (a + b) + c \qquad [2]$$

En efecto: sea C un subconjunto de N al que pertenece c. Para justificar [2], bastará demostrar que $C \equiv N$:

a) $1 \in C$, ya que $a + (b + 1) = a + b^+ = (a + b)^+ = (a + b) + 1$.

b) Siendo $c \in C$, $a + (b + c) = (a + b) + c$
luego:

$$a + (b + c^+) = a + (b + c)^+ = [a + (b + c)]^+ =$$
$$= [(a + b) + c]^+ = (a + b) + c^+;$$

y como $c^+ \in C \Rightarrow C \equiv N$.

2. *Elemento neutro*

Tal como la nota de la página anterior ha establecido el cero, axiomáticamente resulta que

$$\forall a \in N,\ a + 0 = 0 + a = a \qquad [3]$$

3. *Conmutatividad*

$$\forall a,\ b \in N,\ a + b = b + a \qquad [4]$$

En efecto: sea A un subconjunto de N al que pertenece un a que satisface la relación [4]. Para demostrar esa relación, bastará justificar que $A \equiv N$

a) $1 \in A$, puesto que $1 + 1 = 1 + 1$.

b) Siendo $a \in A$, $1 + a = a + 1$,
lo que supone que

$$1 + a^+ = 1 + (a + 1) = (1 + a) + 1 = a^+ + 1$$

c) Finalmente,

$$b + a^+ = b + (a + 1) = (b + a) + 1 = (a + b) + 1 =$$
$$= 1 + (a + b) = (1 + a) + b = a^+ + b;$$

de donde

$$a^+ \in A;$$

luego

$$C \equiv N$$

4. *Ley cancelativa*

$$\forall a,\ b,\ c \in N,\ a + c = b + c \Rightarrow a = b \qquad [5]$$

En efecto: sea C un subconjunto de N al que pertenecen los elementos que satisfacen la relación [5].

a) $1 \in C$, ya que $a + 1 = b + 1 \Rightarrow a^+ = b^+ \underset{(A_4)}{\Rightarrow} a = b.$

b) Si c satisface la ley recién establecida,

$$a + c^+ = b + c^+ \Rightarrow (a + c)^+ = (b + c)^+;$$

y entonces,

$$a + c = b + c \Rightarrow a = b$$

Por ello, c^+ también verifica la [5]. Se concluye, pues, que

$$C \equiv N$$

La bina $[\{N, 0\}, +]$, por obedecer a las leyes primera, segunda y tercera, es un semigrupo abeliano con elemento neutro.

La ley de cancelación (4) es la que permite la simplificación en el semigrupo aditivo de los naturales.

3.1152. *Multiplicación en N*

$$\forall (a, b) \in N \times N,\ \exists^* c \in N / a \cdot b = c \qquad [6]$$

según los siguientes axiomas de definición:

I. $\forall a \in N,\ a \cdot 1 = a.$

II. $a \in N,\ b \in N,\ a \cdot b^+ = a \cdot b + a.$

La expresión [6] indica que la multiplicación así definida es una ley de composición interna u operación en N, cosa que ha de justificarse, basándose en los dos axiomas de definición.

En efecto:

a) sea $B \subset N$ un subconjunto cuyos elementos b verifican que

$$\forall a \in N,\ a \cdot b \in N$$

En particular, como $b \cdot 1 = b \in N \Rightarrow 1 \in B.$

b) Según II,

$$a \cdot b^+ \in N$$

y

$$a \cdot b^+ = a \cdot b + a$$

Como $a \cdot b \in N$, también $a \cdot b^+ \in N$, lo que implica que $b^+ \in C$. Y según A_5,

$$C \equiv N$$

Queda justificado así que la multiplicación en N es una ley de composición interna u operación.

La multiplicación en N obedece a las siguientes leyes:

5. *Asociatividad**

$$\forall a,\ b,\ c \in N,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad [7]$$

En efecto: sea un $C \subset N$ cuyos elementos c satisfacen la relación [7], para todo elemento $a,\ b \in N$.

a) $1 \in C$, ya que $a \cdot (b \cdot 1) = a \cdot b = (a \cdot b) \cdot 1$.
b) Si $c \in C$, entonces

$$\begin{aligned}(a \cdot b) \cdot c^+ &= (a \cdot b) \cdot c + a \cdot b = a \cdot (b \cdot c) + a \cdot b = \\ &= a \cdot [(b \cdot c) + b] = a \cdot (b \cdot c^+);\end{aligned}$$

de donde

$$C \equiv N$$

6. *Elemento unidad*

$$\forall a \in N,\ a \cdot 1 = 1 \cdot a = a \qquad [8]$$

Esta ley descansa directamente sobre el primer axioma definitorio de la operación. La conmutatividad que implica queda justificada en la siguiente ley de

7. *Conmutatividad*

$$\forall a,\ b \in N,\ a \cdot b = b \cdot a \qquad [9]$$

a) $1 \cdot 1 = 1 \cdot 1$.
b) Sea $B \subset N$, cuyos elementos b satisfacen la relación [9], $\forall a \in N$.
Si $b \cdot 1 = 1 \cdot b$, entonces

$$1 \cdot b^+ = b + 1 = b^+ = b^+ \cdot 1$$

---

* Adviértase en la justificación de la ley que se hace uso de la distributividad de la multiplicación respecto de la adición. Una exposición lógica habría de presentar antes la distributividad que la asociatividad.

El orden de exposición establecido obedece exclusivamente a razones de estructuración pedagógica, en conexión con aprendizajes anteriores.

Y también, si $a \cdot b = b \cdot a$, entonces

$$a \cdot b^+ = a \cdot b + a = b \cdot a + a = (b + 1) \cdot a = b^+ \cdot a;$$

luego

$$B \equiv N$$

8. *Ley cancelativa*

$\forall a, b, c \in N$,

$$a \cdot c = b \cdot c \Rightarrow a = b \qquad [10]$$

En efecto: sea C un subconjunto de N al que pertenecen los elementos que satisfacen la relación anterior.

a) $1 \in C$, pues $a \cdot 1 = b \cdot 1 \Rightarrow a = b$.
b) Si $a \cdot c = b \cdot c$, entonces $a \cdot c^+ = b \cdot c^+$; de donde se deduce que

$$b \cdot c^+ + a = b \cdot c^+ + b;$$

y como $a \cdot c = b \cdot c$, la ley 4, cancelativa de la adición exige que

$$a = b;$$

o sea, que

$$C \equiv N$$

La bina $[\{N, 0\}, \cdot]$, por obedecer a las leyes quinta, sexta y séptima, es un semigrupo abeliano con elemento unidad.

La octava ley cancelativa es la base de la simplificación en el semigrupo multiplicativo de los naturales.

Finalmente, una novena ley, referible a ambas operaciones en N, completa su estructura:

9. *Distributividad de la multiplicación respecto de la adición*

$$\forall a, b, c \in N, \ (a + b) \cdot c = a \cdot c + b \cdot c \qquad [11]$$

En efecto: sea $C \subset N$, el conjunto de los elementos c que verifican la relación anterior.

a) $1 \in C$, ya que $(a + b) \cdot 1 = a + b = a \cdot 1 + b \cdot 1$
b) Si se satisface la [11], sucede que

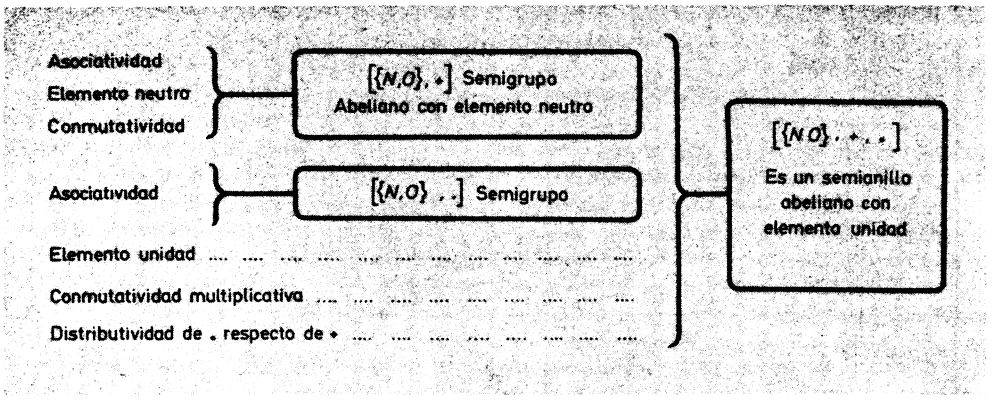
$$(a + b) \cdot c^+ = (a + b) \cdot c + a + b = a \cdot c + b \cdot c + a + b = \\ = (a \cdot c + a) + (b \cdot c + b) = a \cdot c^+ + b \cdot c^+;$$

luego

$$C \equiv N$$

3.1153. *Estructura de* $[\{N, 0\}, +, \cdot]$

Esta última ley referente a ambas operaciones, determina para la terna $[\{N, 0\}, +, \cdot]$ la estructura algebraica que muestra el cuadro.



3.116. Aritmética cardinal

Establecido el conjunto de los números cardinales $\mathfrak{C}$, con su correspondiente estructura de orden, procede ahora establecer su estructura algebraica, mediante la definición en su seno, de dos leyes de composición internas: la adición y la multiplicación.

A la vista del establecimiento de los cardinales finitos (número 3.1135), los conjuntos de cardinales pueden considerarse superconjuntos de aquéllos; y como el conjunto de cardinales finitos es isomorfo con el conjunto de los naturales $\{N, 0\}$, sucede que el establecimiento de la adición y multiplicación en $\mathfrak{C}$ es una generalización de la adición y multiplicación de naturales.

3.1161. *Adición de cardinales*

Sean A, B y C tres conjuntos, tales que

$$A \cap B = \phi$$
$$A \cup B = C;$$

y denotemos

$$\text{card}(A) = a$$
$$\text{card}(B) = b$$
$$\text{card}(C) = c$$

Se dice que la suma de a y b es el cardinal c y se representa

$$a + b = c$$

Obsérvese que, tal como queda definida la adición de cardinales, se trata de una operación uniforme: su resultado c no depende de los representantes de la familia cardinal que se toman para operar. En efecto:

$$A \sim A' \Rightarrow \text{card}(A) = \text{card}(A') = a$$
$$B \sim B' \Rightarrow \text{card}(B) = \text{card}(B') = b$$

Además:

$$A \cap B = \phi; \quad A' \cap B' = \phi$$

y

$$\text{card}(A \cup B) = \text{card}(A' \cup B') = c$$

La adición de cardinales obedece a las leyes que se relacionan, cuya justificación sale directamente de las homónimas de la Teoría de Conjuntos, en que se sustentan. A título recordatorio, se escriben a la derecha de las leyes para cardinales.

1. *Asociatividad*

$$(a + b) + c = a + (b + c) \quad ; \quad (A \cup B) \cup C = A \cup (B \cup C)$$

2. *Elemento neutro*

$$0 + a = a + 0 = a \quad ; \quad \phi \cup A = A \cup \phi = A$$

3. *Conmutatividad*

$$a + b = b + a \quad ; \quad A \cup B = B \cup A$$

La bina $[\mathbb{C}, +]$, por obedecer a las leyes primera, segunda y tercera tiene estructura de semigrupo abeliano con elemento neutro.

3.1162. *Multiplicación de cardinales*

Sean A y B dos conjuntos cuyos cardinales son a y b. Sea p el cardinal del producto cartesiano $A \times B$.

Se define la multiplicación en $\mathbb{C}$ como la operación que hace corresponder a dos cardinales el cardinal de su cartesiano

$$\left.\begin{array}{l} \text{card}(A) = a \\ \text{card}(B) = b \\ A \times B = p \\ \text{card}(P) = p \end{array}\right| \quad a \cdot b = p$$

Resulta inmediato justificar que, por no depender el resultado de los conjuntos representantes escogidos para operar, se trata de una ley uniforme.

La multiplicación de cardinales obedece a las siguientes leyes:

4. *Asociatividad*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad ; \quad A \times (B \times C) = (A \times B) \times C$$

5. *Elemento unidad*

$$a \cdot 1 = 1 \cdot a = a \quad ; \quad A \times \{1\} \neq \{1\} \times A \neq A;$$

pero lo que sí es cierto es que si A tiene de potencia a, el cartesiano $A \times \{1\}$ «tiene» también a pares.

6. *Conmutatividad*

$$a \cdot b = b \cdot a \quad ; \quad A \times B \neq B \times A;$$

aunque la naturaleza de los pares es distinta por tener sus proyecciones en orden inverso, el «número de pares» sí coincide.

La bina $[\mathbb{C}, \cdot]$, por obedecer a las leyes cuarta, quinta y sexta alcanza estructura de semigrupo abelino con elemento unidad.

Finalmente, una séptima ley conexiona ambas operaciones:

7. *Distributividad de la multiplicación respecto de la adición*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad ; \quad A \times (B \cup C) = (A \times B) \cup (A \times C)$$

3.1163. *Estructura de* $[\mathbb{C}, +, \cdot]$

Un cuadro análogo al dispuesto en 3.1153 daría para los cardinales con la adición y multiplicación, una estructura de semianillo abeliano con elemento unidad.

3.1164. *Notación potencial en el conjunto* $\mathbb{C}$

La notación potencial de la Aritmética natural tiene su paralela en el conjunto de los cardinales, en el que se introduce del siguiente modo:

Sean los conjuntos y cardinales que se indican:

$$a = \text{card}(A) \quad ; \quad b = \text{card}(B)$$

La familia de todas las funciones de A en B (véase 2.271) toma la notación

$$B^A;$$

pues bien, se entiende por potencia a de b al cardinal del conjunto de funciones establecido, a saber:

$$b^a = \text{card}(B^A).$$

Así definida la potenciación en $\mathbb{C}$, las reglas de operación de potencias naturales son válidas para el conjunto de cardinales, tales son

$$\begin{aligned} a^b \cdot a^c &= a^{b+c} \\ (a^b)^c &= a^{b \cdot c} \\ (a \cdot b)^c &= a^c \cdot b^c \end{aligned}$$

Compréndase, finalmente, que si se trata de cardinales finitos, b^a denota el mismo número que si a y b fueran naturales.

Ejemplo

Se establecen $A = \{a, b\}$ y $B = \{1, 2, 3\}$, de modo que $\text{card}(A) = 2$ y $\text{card}(B) = 3$ y

$$\text{card}(B^A) = 3^2$$

Establezcamos todas las funciones de la familia B^A:

$$\{(a, 1), (b, 1)\};\ \{(a, 1), (b, 2)\};\ \{(a, 1), (b, 3)\};\ \{(a, 2), (b, 1)\};$$
$$\{(a, 2), (b, 2)\};\ \{(a, 2), (b, 3)\};\ \{(a, 3), (b, 1)\};\ \{(a, 3), (b, 2)\};$$
$$\{(a, 3), (b, 3)\},$$

que han resultado ser nueve. En efecto, tratándose de los cardinales finitos 3 y 2, la potencia cardinal

$$3^2 = 9,$$

como si se tratara de naturales.

3.1165. *Los números naturales y los cardinales*

El hecho de que entre los cardinales finitos y los naturales sea posible establecer un isomorfismo ha inducido, a niveles de estos aprendizajes, a un error suficientemente extendido: el conjunto de los naturales y el de los cardinales es el mismo conjunto. Nada más lejos de la verdad.

Como muestra adviértase, por ejemplo, que mientras que en los naturales se puede simplificar tanto en la adición como en la multiplicación en virtud de sus leyes cancelativas, en los cardinales no siempre esto es posible, como puede comprobarse sobre este caso concreto:

Sean A y B los conjuntos naturales que se expresan:

$$A = \{1, 3, 5, 7, \ldots\} \quad ; \quad B = \{2, 4, 6, \ldots\}$$
$$A \cup B = N \quad ; \quad A \cap B = \phi$$
$$\text{card}(A) = \aleph_0$$
$$\text{card}(B) = \aleph_0$$
$$\text{card}(A \cup B) = \text{card}(N) = \aleph_0$$
$$\aleph_0 + \aleph_0 = \aleph_0 = 1 + \aleph_0 \neq \aleph_0 = 1$$
$$\text{card}(A \times B) = \text{card}(N \times N) = \aleph_0$$
$$\aleph_0 \cdot \aleph_0 = \aleph_0 = 1 \cdot \aleph_0 \neq \aleph_0 = 1$$

3.117. Aritmética ordinal

Establecido el conjunto de los números ordinales $\mathfrak{O}$, con su correspondiente estructura de orden, procede ahora establecer su estructura algebraica, mediante la definición en su seno de dos leyes de composición internas, la adición y la multiplicación.

De un modo similar a lo que sucede con los cardinales, las operaciones de adición y multiplicación de ordinales finitos corresponden a las mismas operaciones en N.

3.1171. *Adición ordinal*

Se establecen los ordinales

$$\lambda = \text{ord}(A) \quad ; \quad \mu = \text{ord}(B)$$

de dos conjuntos disjuntos bien ordenados, $A \cap B = \phi$.

Se define*:

$$\lambda + \mu = \text{ord}(A \dot{+} B)$$

Esta adición de ordinales, así definida, obedece a las siguientes leyes:

1. La adición de ordinales es asociativa

$$\lambda + (\mu + \varphi) = (\lambda + \mu) + \varphi$$

2. Existe el ordinal neutro, 0

$$0 + \lambda = \lambda + 0 = \lambda$$

3. La adición de ordinales no es conmutativa.

El siguiente contraejemplo es suficiente para demostrar la negación del universal

$$\text{ord}(\{1, 2, 3, \ldots\}) = \omega$$
$$\text{ord}(\{a_1, a_2, \ldots, a_n\}) = n$$

Puesto que N es isomorfo a la sección inicial de a_1, $s(a_1)$,

$$\omega + n = \text{ord}(\{1, 2, 3, \ldots, a_1, a_2, \ldots, a_n\}) > \omega$$
$$n + \omega = \text{ord}(\{a_1, a_2, a_3, \ldots, a_n, 1, 2, 3, \ldots\}) = \omega$$
$$\omega + n \neq n + \omega$$

Suma de infinitos ordinales

Es posible realizar la adición de infinitos ordinales, consiguiéndose el resultado

$$\Sigma_{i \in I} \lambda_i = \text{ord}(\bigcup_{i \in I} \{A_i \times \{i\}\}) \qquad [12]$$

Efectivamente: considérese el conjunto de ordinales, bien ordenado, $\{\lambda_i\}_{i \in I}$, lo que quiere significar que I es un conjunto bien ordenado, y que

$$\forall i \in I, \ \exists^* \lambda_i \in \{\lambda_i\}.$$

Entendido que $\lambda_i = \text{ord}(A_i)$, resulta que

$$\{A_i \times \{i\}\}_{i \in I}$$

---

* El símbolo convencional de la reunión $A \dot{+} B$ quiere expresar que el conjunto reunión queda ordenado con los órdenes que tenían A y B y, además, que todo elemento de A precede a todo elemento de B.

Todo en la línea del ejemplo 2 del número 3.1143.

es una familia bien ordenada de conjuntos bien ordenados, disjuntos dos a dos; y entonces la reunión

$$\bigcup_{i \in I} \{A_i \times \{i\}\}$$

es una buena ordenación, lo que permite establecer [12].

Ejemplo

La suma de infinitos ordinales finitos no nulos es el primer ordinal límite

$$\lambda_1 + \lambda_2 + \cdots = \Sigma_{i \in N} \lambda_i = \omega;$$

y en particular se comprueba que

$$1 + 1 + 1 + \cdots = \omega$$

3.1172. *Multiplicación ordinal*

Se establecen los ordinales

$$\lambda = \text{ord}(A) \quad ; \quad \mu = \text{ord}(B)$$

de dos conjuntos A y B.

Se define:

$$\lambda \cdot \mu = \text{ord}(\{A \times B\}),$$

en la que el orden del cartesiano es:

$$\begin{array}{l} (a_1, b_1) \in A \times B \\ (a_2, b_2) \in A \times B \\ (a_1, b_1) < (a_2, b_2) \Rightarrow (a_1 < a_2) \wedge (b_1^- \leq b_2) \end{array}$$

Esta multiplicación de ordinales, así definida, obedece a las siguientes leyes:

4. La multiplicación de ordinales es asociativa

$$\lambda \cdot (\mu \cdot \varphi) = (\lambda \cdot \mu) \cdot \varphi$$

5. Existe el ordinal unidad

$$1 \cdot \lambda = \lambda \cdot 1 = \lambda$$

6. La multiplicación de ordinales no es conmutativa.
Un contraejemplo justifica la negación universal

$$\begin{array}{l} \text{ord}(\{1, 2, 3, \ldots\}) = \omega \\ \text{ord}(\{p, q\}) = 2 \end{array}$$

$$\omega \cdot 2 = \text{ord}(\{(1, p), (2, p), \ldots, (1, q), (2, q), \ldots\}) > \omega,$$

ya que N es isomorfo con la sección inicial $\{(1, p), (2, p), \ldots\}$.
De otro lado,

$$2 \cdot \omega = \text{ord}(\{(p, 1), (q, 1), (p, 2), (q, 2), \ldots, (p, n), (q, n), \ldots\}) = \omega$$

Es claro, pues, que la multiplicación de ordinales no es conmutativa.

7. La multiplicación ordinal es distributiva por la izquierda, respecto de la adición de ordinales.

$$\lambda \cdot (\mu + \varphi) = \lambda \cdot \mu + \lambda \cdot \varphi$$

3.12. EL CONJUNTO *Z*

3.121. Necesidad de ampliar *N*

En el semigrupo aditivo de los naturales $[\{N, 0\}, +]$ no siempre tiene solución la ecuación

$$a + x = b \qquad [13]$$

Si $b < a$, no existe ningún $x \in N$ que satisfaga la igualdad establecida. Con el fin de conseguir que la ecuación [13] tenga siempre solución, se crea un nuevo conjunto de números en el que la diferencia siempre es posible.

El proceso consiste en simetrizar el semigrupo abeliano $[\{N, 0\}; +]$, creando el grupo conmutativo $[Z, +]$.

(Véase el desarrollo completo y generalizado de esta técnica en el número 2.43.)

3.122. Simetrización del semigrupo abeliano cancelativo [{N, 0}, +]

3.1221. *Condiciones de simetrización*

Según quedó expresado en el número 2.4321, para que un semigrupo sea simetrizable es necesario que

a) sea conmutativo,
b) obedezca a la ley cancelativa y, por tanto, sea posible la simplificación.

Ambas condiciones las cumple el semigrupo $[\{N, 0\}; +]$:

a) $a + b = b + a, \quad \forall a, b \in N$
b) $a + c = b + c \Rightarrow a = b, \quad \forall a, b, c \in N$

3.1222. *Relación de equivalencia sobre N^2, agente de clasificación*

A) *Establecimiento de R*

$\forall (a, b) \in N^2, \quad \forall (c, d) \in N^2,$

$$(a, b) \equiv (c, d) \Leftrightarrow a + d = b + c$$

B) *Análisis de R.* La relación establecida es de equivalencia. En efecto:

B_1) *Reflexividad*

Por ser $[\{N, 0\}, +]$ abeliano,

$$a + b = b + a \Leftrightarrow (a, b) \equiv (a, b), \qquad \forall (a, b) \in N^2$$

B_2) *Simetría*

$$\begin{array}{l} (a, b)\ ,\ (c, d) \in N^2, \\ (a, b) \equiv (c, d) \Rightarrow (c, d) \equiv (a, b) \\ \Updownarrow \\ a + d = b + c \\ \Downarrow \\ a + d = c + b \\ \Downarrow \\ c + b = a + d \Leftrightarrow (c, d) \equiv (a, b) \end{array}$$

B_3) *Transitividad*

$$\begin{array}{l} (a, b),\ (c, d),\ (e, f) \in N^2, \\ \left.\begin{array}{l} (a, b) \equiv (c, d) \\ (c, d) \equiv (e, f) \end{array}\right\} \Rightarrow (a, b) \equiv (e, f) \\ \hline \left.\begin{array}{l} (a, b) \equiv (c, d) \Leftrightarrow a + d = b + c \\ (c, d) \equiv (e, f) \Leftrightarrow c + f = d + e \end{array}\right\} + \\ (a + d) + (c + f) = (b + c) + (d + e) \\ \Downarrow \quad \text{Asociatividad} \\ a + d + c + f = b + c + d + e \\ \Downarrow \quad \text{Cancelación} \\ (a + f) = (b + e) \\ \Updownarrow \\ (a, b) \equiv (e, f) \end{array}$$

C) *Acción de R sobre* N^2

R clasifica y parte a N^2 en clases de equivalencia, que son elementos del conjunto cociente

$$\begin{array}{l} Z = N^2/R = \{\{\alpha\}, \{\beta\}, \{\gamma\}, \ldots\} \\ \{\alpha\} = \{(a_1, b_1) \equiv (a_2, b_2) \equiv \ldots\} \\ \{\beta\} = \{(c_1, d_1) \equiv (c_2, d_2) \equiv \ldots\} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Z es el denominado conjunto de los enteros relativos.

3.1223. *Representantes canónicos. Enteros positivos, negativos y nulo*

Considérense los números enteros

$$\begin{array}{l} \{\alpha\} = \{(10, 8) \equiv (4, 2) \equiv (7, 5) \equiv (2, 0) \equiv \ldots\} \\ \{\beta\} = \{(4, 7) \equiv (6, 9) \equiv (1, 4) \equiv (0, 3) \equiv \ldots\} \\ \{\gamma\} = \{(5, 5) \equiv (3, 3) \equiv (2, 2) \equiv (0, 0) \equiv \ldots\} \end{array}$$

Para manejar números enteros, es conveniente ponerse de acuerdo, para tomar como representantes de ellos el par más sencillo de la clase.

Se conviene en llamar representante canónico de un entero al par de su clase que tiene una, otra o las dos proyecciones nulas. Así, se dirá que el entero

$$\alpha = \{(2, 0)\}$$
$$\beta = \{(0, 3)\}$$
$$\gamma = \{(0, 0)\}$$

Todavía, como puede entenderse, resulta engorrosa la notación y, cuando la simplificación de escritura no resulta ambigua, se permiten los siguientes simbolismos simplificativos:

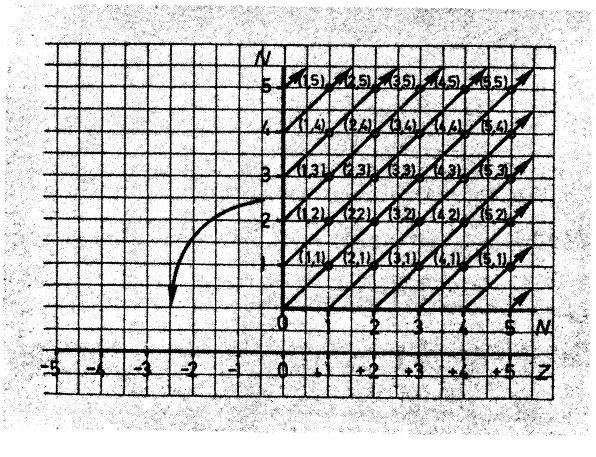
$$\alpha = \{(2, 0)\} = (2, 0) = (+2) = +2$$
$$\beta = \{(0, 3)\} = (0, 3) = (-3) = -3$$
$$\gamma = \{(0, 0)\} = (0, 0) = (0) = 0$$

Pero adviértase que los signos + y − utilizados, en modo alguno son operativos; son simplemente *atributivos*, indicando cuál de las dos proyecciones del canónico es nula.

De este modo, el conjunto de los enteros Z ha quedado clasificado en tres subconjuntos disjuntos, que son:

Z^+: el conjunto de los enteros positivos, del tipo $(+a)$;
Z^-: el conjunto de los enteros negativos, del tipo $(-b)$;
0: el conjunto unitario de los enteros nulos (0, 0).

La figura adjunta muestra dos modos tradicionales de representar gráficamente el conjunto Z. Las «diagonales» del cuadro cartesiano representan las clases enteras; abatiendo el eje de ordenadas, se consigue la representación en la recta.



3.1224. *Adición inducida en Z*

Creado el conjunto Z a partir de N^2, mediante la relación de equivalencia descrita, observemos qué ha sucedido con la adición en N.

Es inmediatamente justificable que la adición de naturales es estable frente a la relación de equivalencia que define Z y, por tanto, induce una ley de composición interna entre las clases de N^2/R. (Consúltese el número 2.34.)

$$\forall\{(a, b)\} \in Z, \quad \forall\{(c, d)\} \in Z$$
$$\{(a, b)\} \hat{+} \{(c, d)\} = \{(a + c,\ b + d)\}$$

De este modo queda establecida la adición en Z.

Con el artificioso signo $\hat{+}$ se ha querido resaltar que la naturaleza de la operación es distinta que la de N. Entendemos que es suficiente y, a partir de ahora, la adición en Z se denotará también con el signo simple $+$.

3.123. El grupo aditivo de los enteros relativos Z

La bina $[Z, +]$ tiene estructura de grupo abeliano. En efecto:

0. *Uniformidad.* La ley $+$ es cerrada en Z; es decir, el resultado pertenece a Z y es único.

   Justificación: La ley $+$ lo es en N y queda dicho que es estable frente a la relación R que define Z.

1. *Asociatividad.*

$$\{(a, b)\} + [\{(c, d)\} + \{(e, f)\}] = [\{(a, b)\} + \{(c, d)\}] + \{(e, f)\}$$

   Justificación: Basta operar ambos miembros y constatar resultados iguales.

2. *Existencia de elemento neutro*

$$\{(a, b)\} + \{(n, n)\} = \{(n, n)\} + \{(a, b)\} = \{(a, b)\}$$

   Justificación:

$$a + (n + b) = b + (n + a)$$
$$\Downarrow$$
$$\{(a, b)\} = \{(n + a, n + b)\} = \{(n, n)\} + \{(a, b)\}$$

3. *Elementos opuestos*

$$\{(a, b)\} + \{(b, a)\} = \{(a + b,\ b + a)\} = \{(a + b,\ a + b)\} \equiv \{(n, n)\}$$

4. *Conmutatividad*

$$\{(a, b)\} + \{(c, d)\} = \{(c, d)\} + \{(a, b)\}.$$

   En efecto:

$$\{(a, b)\} + \{(c, d)\} = \{(a + c,\ b + d)\} = \{(c + a,\ d + b)\} = \{(c,\ d)\} + \{(a, b)\}$$

3.124. El semigrupo [N, +] sumergido en el grupo [Z, +]

Considérense, $\forall a \in N$, los pares del cartesiano N^2, del tipo $(a + x, x)$, $\forall x \in N$.

Intentemos demostrar que todos los pares de la forma establecida pertenecen a la misma clase de $N^2/R = Z$. En efecto:

$$\underline{(a + x) + y} = a + (x + y) = (a + y) + x = \underline{x + (a + y)}$$
$$\Updownarrow$$
$$(a + x,\ x) \equiv (a + y,\ y)$$

Recíprocamente, si

$$(a + x, x) \equiv (p, q) \Rightarrow p = a + q.$$

En efecto:

$$(a + x, x) \equiv (p, q) \Rightarrow (a + x) + q = x + p \Rightarrow a + x + q = x + p \Rightarrow a + q = p$$

Se establece ahora la aplicación f de N en Z, con el siguiente criterio:

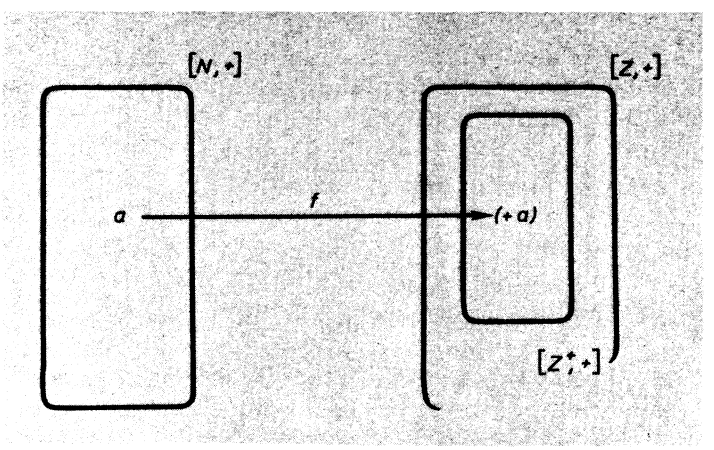
$$N \xrightarrow{f} Z$$
$$a \longrightarrow f(a) = \{(a + x, x)\}$$

de modo que a cada elemento de N le corresponde como imagen la clase de N^2/R, anteriormente establecida.

Un inmediato análisis de f nos dice que es una inyección y un homomorfismo; en fin, la f establecida en un monomorfismo.

Por último, si se restringe el monomorfismo f al subconjunto de $N^2/R = Z$, formado por las imágenes de N, aparece un monomorfismo epimórfico, es decir, un isomorfismo.

Tal isomorfismo es el que denominamos «isomorfismo de inmersión» que, de algún modo, permite «sumergir» el conjunto N en Z, como subconjunto suyo. En realidad, se insiste, lo que se hace es homologar N a su conjunto imagen Z^+, isomórfico en $N^2/R \to Z$.



3.125. Orden en [Z, +]

Sea la relación en Z

$$a \leq b \Leftrightarrow b - a \in \{Z^+, 0\} \qquad [14]$$

La relación [14] es

Reflexiva: $a - a = 0 \in \{Z^+, 0\} \Rightarrow a \leq a$

Antisimétrica: $\left.\begin{array}{l} a \leq b \Rightarrow b - a \in \{Z^+, 0\} \Rightarrow b - a \in \{0\} \\ b \leq a \Rightarrow a - b \in \{Z^+, 0\} \Rightarrow a - b \in \{0\} \end{array}\right\} \Rightarrow a = b$

Transitiva: $\left.\begin{array}{l} a \leq b \Rightarrow b - a \in \{Z^+, 0\} \\ b \leq c \Rightarrow c - b \in \{Z^+, 0\} \end{array}\right\} \Rightarrow c - a \in \{Z^+, 0\} \Rightarrow a \leq c$

Se trata, pues, de una relación de orden amplio; además:

$$\forall a, b \in Z, \ (a \leq b) \vee (b \leq a)$$

pues

$$b - a \in \{Z^+, 0\} \Rightarrow a \leq b$$

o bien

$$b - a \in \{Z^-, 0\} \Rightarrow (a - b) \in \{Z^+, 0\} \Rightarrow b \leq a$$

Con ello, queda establecido $[Z, \leq]$ como un orden amplio total.

Por otra parte,

$$\forall a, b, c \in Z, \ b - a \in \{Z^+, 0\} \Rightarrow b - a = b + c - (a + c) \in \{Z^+, 0\},$$

lo que significa que la relación establecida es compatible con la operación del grupo.

Finalmente,

$$\forall a, b \in Z^+, \ \exists c \in Z^+ / c \cdot a > b \qquad [15]$$

En efecto: por ejemplo, si $c = b + 1$,

$$(b + 1) \cdot a = b \cdot a + a \geq b + a \geq b + 1 > b$$

Por cumplirse [15], se dice que se trata de un orden arquimediano.

Reuniendo todos los resultados del análisis, se concluye: $[Z, +, \leq]$ es un grupo totalmente ordenado arquimediano.

3.126. La multiplicación en Z

Se establece la aplicación

$$Z \times Z \xrightarrow{\times} Z$$

$$(\{(a, b)\}, \{(c, d)\}) \longrightarrow \{(a, b)\} \times \{(c, d)\} = \{(a \cdot c + b \cdot d, \ b \cdot c + a \cdot d)\}$$

La artificiosidad de esta definición de producto de enteros se justifica porque, de ese modo, se consigue una ley de composición interna en Z, que es una inducción de la multiplicación en N.

Antes de nada, justifiquemos la uniformidad de la ley demostrando que es estable frente a la relación de equivalencia que definió Z a partir de N^2.

Sean dos enteros

$$\alpha = \{(a_1, b_1) \equiv (a_2, b_2) \equiv \ldots\}$$
$$\beta = \{(c_1, d_1) \equiv (c_2, d_2) \equiv \ldots\}$$

Se procede a su multiplicación usando unos u otros de sus pares representantes. Si se consiguen idénticos resultados, se habrá demostrado la estabilidad de la ley.

$$(a_1, b_1) \equiv (a_2, b_2) \Leftrightarrow a_1 + b_2 = b_1 + a_2 \qquad [16]$$
$$(c_1, d_1) \equiv (c_2, d_2) \Leftrightarrow c_1 + d_2 = d_1 + c_2 \qquad [17]$$

Operando como se indica, y advirtiendo que la segunda y cuarta multiplicaciones se han dispuesto sobre las igualdades simétricas, se establece:

$$\left.\begin{array}{l} [16] \times c_1 : a_1c_1 + b_2c_1 = b_1c_1 + a_2c_1 \\ [16] \times d_1 : b_1d_1 + a_2d_1 = a_1d_1 + b_2d_1 \\ [17] \times a_2 : c_1a_2 + d_2a_2 = d_1a_2 + c_2a_2 \\ [17] \times b_2 : d_1b_2 + c_2b_2 = c_1b_2 + d_2b_2 \end{array}\right\} +$$
$$a_1c_1 + b_1d_1 + a_2d_2 + b_2c_2 = b_1c_1 + a_1d_1 + a_2c_2 + b_2d_2 \qquad [18]$$

La igualdad [18] implica la siguiente igualdad de pares:

$$(a_1c_1 + b_1d_1,\ b_1c_1 + a_1d_1) \equiv (a_2c_2 + b_2d_2,\ a_2d_2 + b_2c_2)$$
$$\Updownarrow$$
$$(a_1, b_1) \times (c_1, d_1) = (a_2, b_2) \times (c_2, d_2), \qquad \text{c.q.d.}$$

La multiplicación de enteros obedece a las siguientes leyes:

5. *Asociatividad*

$$[\{(a, b)\} \cdot \{(c, d)\}] \cdot \{(e, f)\} = \{(a, b)\} \cdot [\{(c, d)\} \cdot \{(e, f)\}]$$

Basta operar ambos miembros, para justificar la ley.

6. *Existencia de elemento unidad*

$$\forall \{(a, b)\} \in Z,\ \exists^* \{(1, 0)\} \in Z / \{(a, b)\} \cdot \{(1, 0)\} = \{(1, 0\} \cdot \{(a, b)\} = \{(a, b)\}$$

Es suficiente operar, para comprobarlo.

7. *Conmutatividad*

$$\{(a, b)\} \cdot \{(c, d\} = \{(c, d)\} \cdot \{(a, b)\}$$

Muéstrese, operando, que la igualdad expuesta es correcta.

La bina $[Z, \cdot]$, por cumplir las leyes quinta, sexta y séptima, alcanza la estructura de semigrupo abeliano con elemento unidad.

Además:

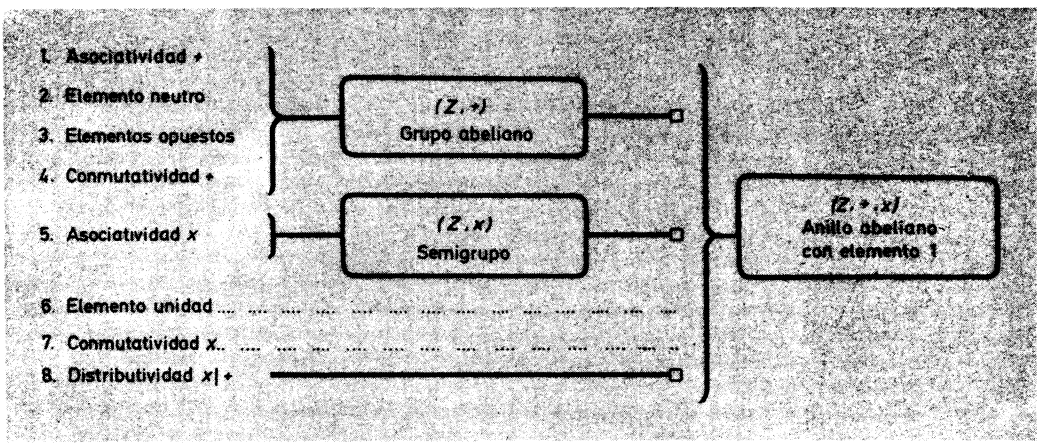
8. *Distributividad de la multiplicación respecto de la adición*

$$\{(a, b)\} \cdot [\{(c, d)\} + \{(e, f)\}] = \{(a, b)\} \cdot \{(c, d)\} + \{(a, b)\} \cdot \{(e, f)\}$$

Realícese el ejercicio de operar ambos miembros y constatar idénticos resultados.

3.127. El anillo multiplicativo de los enteros relativos

El esquema que se realiza describe cómo el conjunto Z, dotado de las operaciones de adición y multiplicación definidas, alcanza la estructura de anillo abeliano con elemento unidad.



3.128. El anillo ordenado $[Z, +, \times]$

Establecida en 3.125 la relación de orden en Z y, visto que es compatible con la adición, procede ahora analizar su comportamiento, respecto de la multiplicación.

$$(a \geq 0) \wedge (b \geq 0) \Rightarrow a \cdot b \geq 0,$$

lo que implica que

$$(a \leq b) \wedge (c \geq 0) \Rightarrow (b - a) \cdot c \geq 0;$$

es decir:

$$a \cdot c \leq b \cdot c$$

Queda así justificado que la relación de orden establecida en Z es compatible con la multiplicación. Por eso, uniendo conclusiones, se puede afirmar que $[Z, +, \times, \leq]$ es un anillo totalmente ordenado arquimediano.

3.129. Divisibilidad en Z

3.1291. *Relación de divisibilidad*

Se establece sobre Z la relación de divisibilidad, denotada x/y y leída indistintamente «x divide a y» o «x es divisor de y», mediante la equivalencia

$$x \in Z^0,\ y \in Z,\ x/y \Leftrightarrow \exists^* c \in Z \,/\, y = x \cdot c$$

(Se ha signado $Z^o = Z - \{0\}$.)

La relación establecida es reflexiva y transitiva, pero no es antisimétrica. En efecto:

1) *Reflexiva*:

$$x/x,\ \forall x \in Z, \qquad \text{ya que } x = x \cdot 1$$

2) *Transitiva*:

$$\left.\begin{matrix} x/y \\ y/z \end{matrix}\right\} \Rightarrow x/z$$

$$x/y \Leftrightarrow y = x \cdot c \qquad [19]$$

$$y/z \Leftrightarrow z = y \cdot d \qquad [20]$$

Sustituyendo [19] en [20],

$$z = x \cdot c \cdot d = x \cdot (c \cdot d) \Leftrightarrow x/z$$

3) No es *antisimétrica*, ya que, si

$$(x/y) \wedge (y/x) \not\Rightarrow x = y,$$

sino que pueden suceder dos cosas: $x = \pm y$.

Tras el análisis realizado, resulta que la relación de divisibilidad en Z no es de orden, sino solamente una preordenación (véase 1.342).

3.1292. *División euclídea*

$$\forall (a, b) \in Z \times Z^+,\ \exists^* (q, r) \in Z \times Z \,/\, (a = b \cdot q + r) \wedge (0 \leq r < b) \quad [21]$$

Reconózcase en a, b, q y r el dividendo, divisor, cociente y resto, respectivamente, de la operación de división.

La [21] constituye un teorema que se pasa a demostrar.

1) Probemos que q siempre existe

1-*a*) *si* $a \geq 0$: $a = b \cdot q + r \Rightarrow b \cdot q \leq a$.
Quedó probado, al establecer el orden arquimediano en Z^+, que siempre existe un q que satisface la desigualdad propuesta;

1-*b*) *si* $a < 0$: entonces, $-a \in Z^+$ y existe un $q' \in Z^+$, tal que

$$b \cdot q' \leq -a < b \cdot (q' + 1);$$

si $b \cdot q' = -a$, basta tomar $q = -q'$ para tener $b \cdot q = a$; si $b \cdot q' < -a$, se establece $q = -(q' + 1)$, con lo que

$$-b \cdot (q + 1) < -a < -b \cdot q$$

2) Justifiquemos que q es único.
En efecto: establecido el dividendo a y el divisor b, sea el subconjunto de Z

$$A = \{x/(x \in Z) \wedge (x \cdot b \leq a)\}$$

En el orden $[A, \leq]$, q resulta ser último elemento y, por tanto, único.
Consecuencias inmediatas del teorema de la división euclídea son:

a) $0 \leq r < b$;
b) si $r = 0 \Rightarrow b/a$ y q es, entonces, el llamado cociente exacto de a y b;
c) si $c \in Z^+$, multiplica al dividendo y al divisor, también multiplica al resto:

$$a \cdot c = (b \cdot c) \cdot q + r \cdot c \qquad 0 \leq r \cdot c < b \cdot c$$

d) si $d \in Z^+$, es divisor común al dividendo y al divisor, también divide al resto: siendo

$$\begin{gathered} a = a' \cdot \mathrm{d} \\ b = b' \cdot \mathrm{d}, \\ r = a - b \cdot q = (a' - b' \cdot q) \cdot d = r' \cdot d \end{gathered}$$

3.1293. *Relación de congruencia, módulo m*

Se establece sobre Z la siguiente relación:

$$a \equiv b \ (m \Leftrightarrow m/(a - b), m \in Z^+ \qquad [22]$$

que se lee: «a es congruente con b, módulo m, si y solamente si, el módulo estrictamente positivo es divisor de la diferencia $(a - b)$».

La relación [22] es de equivalencia. En efecto:
Reflexividad:

$$\forall x \in Z, \ x - x = 0, \ m/0, \ \forall m \in Z^+ \Leftrightarrow a = a \ (m$$

Simetría:

$$\begin{gathered} x, y \in Z, \ x \equiv y \ (m \Rightarrow m/(x - y) \Leftrightarrow x - y = km \Rightarrow \\ \Rightarrow y - x = (-k) \cdot m \Rightarrow m/(y - x) \Leftrightarrow y \equiv x \ (m \end{gathered}$$

Transitividad:

$$x, y, z \in Z,$$

$$\left.\begin{array}{l} x \equiv y \ (m \Leftrightarrow m/(x - y) \Leftrightarrow x - y = p \cdot m \\ y \equiv z \ (m \Leftrightarrow m/(y - z) \Leftrightarrow y - z = q \cdot m \end{array}\right\} +$$

$$x - z = (p + q) \cdot m \Leftrightarrow m/(x - z) \Leftrightarrow x \equiv z \ (m$$

Como tal relación de equivalencia, la relación de congruencia clasifica y parte al conjunto de los enteros en clases, llamadas residuales, por la razón que se expresa:

Sean los enteros x e y, tales que

$$\left.\begin{array}{l} x = m \cdot p + r \\ y = m \cdot q + r \end{array}\right\} -$$

$$x - y = m(p - q) = m \Leftrightarrow m/(x - y) \Leftrightarrow x \equiv y \,(m \qquad [23]$$

La [23] indica que, si como se ha establecido, dos enteros dan el mismo resto al dividirlos por un módulo m, son congruentes, módulo m.

De otro lado, si es r el resto de la división de un entero x por un módulo m, sucede que x y r son, a su vez, congruentes respecto de ese módulo:

$$x = m \cdot p + r$$
$$x - r = m \cdot p + r - r = m \cdot p \Leftrightarrow x \equiv r \,(m$$

Así, pues, x, y, r son tres elementos de la misma clase de congruencia

$$Z/m = \{\{x \equiv y \equiv r \equiv \ldots\}, \{\ldots\}, \ldots\}$$

A la hora de convenir un elemento canónico para que represente a cada una de las clases de congruencia, parece lógico usar el menor de ellos. Pues bien: éste siempre es el resto; de ahí el nombre de «clases residuales» que anteriormente se les ha dado.

Finalmente, teniendo en cuenta que $r < m$, sucede que el conjunto de las clases residuales Z/m es un conjunto finito de m elementos, que son:

clase $\{0\}$: $\quad \forall x \in Z = \dot{m}$
clase $\{1\}$: $\quad \forall x \in Z/x = p \cdot m + 1$
clase $\{2\}$: $\quad \forall x \in Z/x = p \cdot m + 2$
. . . . . .
. . . . . .
clase $m - 1$: $\quad \forall x \in Z/x = p \cdot m + (m - 1)$

Ejemplo

El conjunto de las clases residuales módulo 5 es:

$$Z/5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Una de tantas formas de indicar las clases es «tildar» los restos, que es la que se ha elegido.

Todos los $\dot{5} \in \bar{0}$, ya que $\dot{5} = 5 \cdot k + 0$.

Todos los $x \in Z$ de la forma $(\dot{5} + 1) \in \bar{1}$, pues

$$(\dot{5} + 1) = 5 \cdot q + 1;$$

y también

$$(\dot{5} + 2) \in \bar{2} \quad ; \quad \dot{5} + 2 = 5 \cdot p + 2$$
$$(\dot{5} + 3) \in \bar{3} \quad ; \quad \dot{5} + 3 = 5 \cdot t + 3$$
$$(\dot{5} + 4) \in \bar{4} \quad ; \quad \dot{5} + 4 = 5 \cdot s + 4$$

Así, pues, las m clases del conjunto de las clases residuales módulo m toman la expresión general

$$Z/m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$$

La adición y multiplicación en Z son estables frente a la relación de equivalencia que define Z/m y, por tanto, induce en el conjunto de las clases residuales otras dos operaciones, que denominaremos también adición y multiplicación de residuales:

$$\bar{a} + \bar{b} = \overline{a+b} \quad ; \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Sendas operaciones obedecen a las leyes que se expresan. Su justificación no ofrece dificultad alguna y constituye un buen ejercicio para el lector.

1) *Asociatividad*

$$\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c} \quad ; \quad \bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$

2) *Elemento neutro* *elemento unidad*

$$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a} \quad ; \quad \bar{a} \cdot \bar{1} = \bar{1} \cdot \bar{a} = \bar{a}$$

3) *Elementos opuestos*

$$\bar{a} + \overline{m-a} = m \in \bar{0}$$

4) *Conmutatividad*

$$\bar{a} + \bar{b} = \bar{b} + \bar{a} \quad ; \quad \bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$$

$[Z/m, +]$ tiene estructura de grupo abeliano.

$[Z/m, \times]$ alcanza estructura de semigrupo abeliano con elemento 1.

5) *Distributividad de la multiplicación respecto de la adición*

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

$[Z/m, +, \times]$ presenta estructura de anillo abeliano con elemento unidad.

3.1294. *Divisibilidad e ideales en Z*

Antes de nada se aconseja al lector que relea en los números 2.651 y 2.654 los conceptos de ideal principal e ideal primo.

Se inicia este epígrafe con el siguiente

TEOREMA. Todo ideal de Z es principal. En efecto: se establece la función

$$\begin{array}{c} Z \xrightarrow{f} Z^+ \cup \{0\} \\ x \longrightarrow f(x) = +x \end{array}$$

Sea

$$a \in I \,/\, (x \in I) \Rightarrow f(a) \leq f(x),\ f(a) \in Z^+$$

Sucede que

$$\left.\begin{array}{l} x = q \cdot a + r,\ f(r) < f(a) \\ a \in I \ \Rightarrow q \cdot a \in I \\ \left.\begin{array}{l} x \in I \\ q \cdot a \in I \end{array}\right\} \Rightarrow x - q \cdot a = r \in I \\ \left.\begin{array}{l} f(r) < f(a) \\ f(a \text{ mínimo} \end{array}\right\} \Rightarrow f(r) = 0; \end{array}\right. \qquad [24]$$

pero

$$f(r) = |r| = 0 \Rightarrow r = 0;$$

luego la [24] queda reducida a $x = q \cdot a$.

Ello significa que

$$I \subset (a) \qquad [25]$$

signando (a) ideal principal de base a.

Como por otra parte

$$(a) \subset I, \qquad [26]$$

de [25] y [26] se concluye $I \equiv (a)$.

Adición de ideales

Conviene establecer ahora el concepto de adición de ideales. Sobre el conjunto de ideales $\mathscr{Y}$ de un anillo A, se establece la función

$$\begin{array}{l} \mathscr{Y} \times \mathscr{Y} \xrightarrow{+} \mathscr{Y} \\ (I_1, I_2) \longrightarrow I_1 + I_2 = I, \end{array}$$

del siguiente modo:

$$\forall x \in I_1,\ \forall y \in I_2,\ \exists^* I = I_1 + I_2 / x + y = z \in I$$

Justifiquemos que, en efecto, el resultado de la adición de ideales es otro ideal.

Siendo $x,\ x' \in I_1\ ;\ y,\ y' \in I_2$,

$$u,\ v \in I_1 + I_2 \Leftrightarrow (u = x + y) \wedge (v = x' + y');$$

luego

$$u - v = (x + y) - (x' + y') = (x - x') + (y - y') \in I_1 + I_2.$$

Además, si

$$(u \in I_1 + I_2) \wedge (v \in A),$$

entonces

$$u = x + y,\ (x \in I_1) \wedge (y \in I_2)$$

de donde

$$v \cdot u = v \cdot (x + y) = v \cdot x + v \cdot y \in I_1 + I_2, \qquad \text{c.q.d.}$$

En particular, si se trata del anillo Z, como todos sus ideales son principales, sucede que la suma de dos de ellos produce otro ideal principal de Z.

Máximo común divisor de dos enteros

Sean (a) y (b) dos ideales de Z, de modo que

$$(a) + (b) = (d)$$

Es claro que $(a) \subset (d)$ y que $(b) \subset (d)$ y, por tanto, se puede escribir:

$$a', b' \in Z\,,\ a = a' \cdot d\,,\ b = b' \cdot d \qquad [27]$$

La [27] expresa que d es un divisor común de a y b.

De otro lado, es evidente que

$$d \in (a) + (b),$$

lo que permite escribir que

$$p,\ q \in Z,\ d = p \cdot a + q \cdot b \qquad [28]$$

La expresión [28] indica que todo divisor común de a y de b lo es también de d; o lo que es igual, que d es el máximo común divisor de a y de b.

Algoritmo de Euclides

$$a, b \in Z,\ b < a,\ a = q_0 \cdot b + r_0,\ f(r) < f(b),\ f(r) \neq 0$$

despejando,

$$r_0 = a + (-q_0) \cdot b \in (a) + (b)$$

$$b = q_1 \cdot r_0 + r_1\,,\ f(r_1) < f(r_0)\,,\ f(r_1) \neq 0;$$

y despejando,

$$r_1 = b + (-q_1) \cdot r_0 \in (a) + (b).$$

De este modo, ya que $f(b) > f(r_0) > f(r_1) > \ldots$, se llegaría, tras un número finito de divisiones, a una imagen $f(r_n) = 0 \Rightarrow r_n = 0$. Eso sucedería en la división

$$\begin{array}{c|c} r_{n-2} & r_{n-1} \\ \hline r_n = 0 & q_n \end{array} \Leftrightarrow$$

$$\Leftrightarrow r_{n-2} = q_n \cdot r_{n-1} + r_n = q_n \cdot r_{n-1}$$

Quiere decirse, entonces, que $r_{n-2} \in (r_{n-1})$.

La anterior división es

$$\begin{array}{c|c} r_{n-3} & r_{n-2} \\ \hline r_{n-1} & q_{n-1} \end{array} \Leftrightarrow r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1},$$

lo que supone que $r_{n-3} \in (r_{n-1})$.

Todo sucede igual hasta llegar a la primera, en la que

$$a \in (r_{n-1}).$$

De ello se deduce que

$$(a) + (b) \subset (r_{n-1}) \qquad [29]$$

Ahora se trata de justificar la inclusión recíproca de la [29]. Para ello,

$$\begin{aligned} r_{n-1} &= r_{n-3} + (-q_{n-1}) \cdot r_{n-2} \\ r_{n-2} &= r_{n-4} + (-q_{n-2}) \cdot r_{n-3} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ r_1 &= b + (-q_1) \cdot r_0 \\ r_0 &= a + (-q_0) \cdot b \end{aligned}$$

Sustituyendo sucesivamente cada una de estas igualdades en la anterior, se alcanza para r_{n-1} la expresión

$$r_{n-1} = p \cdot a + q \cdot b \Rightarrow r_{n-1} \in (a) + (b);$$

o sea:

$$(r_{n-1}) \subset (a) + (b) \qquad [30]$$

Las dos soluciones, [29] y [30], permiten escribir

$$(r_{n-1}) = (a) + (b)$$

Si esto es así, se concluye que el resto r_{n-1} es el máximo común divisor de a y de b:

$$d \equiv r_{n-1}$$

Ejemplo

Calcúlese el máximo común divisor de 126 y 93. Determínense también los enteros p y q que verifican la igualdad

$$d = 126p + 93q$$

	1	2	1	4	2
126	93	33	27	6	3
33	27	6	3	0	

$$d(126, 93) = 3$$

$$3 = 126p + 93q, \; p, \; q \in Z$$

$$3 = 27 - 4 \cdot 6 = 27 - 4(33 - 27) =$$
$$= 5 \cdot 27 - 4 \cdot 33 = 5 \cdot (93 - 2 \cdot 33) - 4 \cdot 33 =$$
$$= 5 \cdot 93 - 14 \cdot 33 = 5 \cdot 93 - 14(126 - 93) =$$
$$= 19 \cdot 93 - 14 \cdot 126$$
$$p = -14; \quad ; \quad q = 19$$

Intersección de ideales

Sobre el conjunto de ideales $\mathscr{Y}$ de un anillo A se establece la función

$$\mathscr{Y} \times \mathscr{Y} \xrightarrow{\cap} \mathscr{Y}$$
$$(I_1, I_2) \longrightarrow I_1 \cap I_2 = I,$$

del siguiente modo:

$$x \in I \Leftrightarrow (x \in I_1) \wedge (x \in I_2).$$

Se trata, pues, de la intersección de los dos conjuntos que son ideales.

Demostremos que, en efecto, el resultado de la intersección de dos ideales es otro ideal

1) $x, y \in I \Leftrightarrow (x, y \in I_1) \wedge (x, y \in I_2)$
$$\Downarrow \qquad\qquad \Downarrow$$
$$(x - y \in I_1) \wedge (x - y \in I_2)$$
$$\Downarrow$$
$$(x - y) \in I$$

2) $(x \in I) \wedge (y \in A) \Leftrightarrow (x \in I_1) \wedge (x \in I_2) \wedge (y \in A).$

Entonces,

$$(x \cdot y \in I_1) \wedge (x \cdot y \in I_2)$$
$$\Downarrow$$
$$x \cdot y \in I = I_1 \cap I_2$$

En particular, si se trata del anillo Z, como todos sus ideales son principales, sucede que la intersección de dos de ellos produce otro ideal principal en Z.

Mínimo común múltiplo de dos enteros

Sean (a) y (b) dos ideales de Z, de modo que

$$(a) \cap (b) = (M)$$

Es claro que

$$[(M) \subset (a)] \wedge [(M) \subset (b)]$$

y, por tanto, se puede escribir:

$$(M = m \cdot a) \wedge (M = n \cdot b) \qquad [31]$$

La [31] expresa que M es un múltiplo común de a y de b.

Sea s otro múltiplo común de a y b; entonces,

$$(s = i \cdot a) \wedge (s = j \cdot b),$$

lo que supone que

$$s \in (a) \cap (b) = (M)$$
$$\Downarrow$$
$$s = k \cdot M$$

Es evidente, pues, que de todos los múltiplos comunes a a y a b, M es el menor.

$$M = \text{m.c.m.}(a, b)$$

El cálculo del mínimo común múltiplo resulta ser el siguiente:

$$\begin{aligned} M &= m \cdot a = n \cdot b \\ m \cdot a' \cdot d &= n \cdot b' \cdot d \\ m \cdot a' &= n \cdot b' \end{aligned} \qquad [32]$$

De otro lado, a' y b' son números sin ningún divisor común, lo que hace que la [28] tome para ellos la siguiente forma:

$$1 = p \cdot a' + q \cdot b' \qquad [33]$$

Multiplicando por m,

$$\begin{aligned} m &= p \cdot a' \cdot m' + q \cdot b' \cdot m \\ m &= p \cdot n \cdot b' + q \cdot m \cdot b' \\ m &= (p \cdot n + q \cdot m) \cdot b' \\ m &= k \cdot b'; \end{aligned}$$

Sustituyendo en [32],

$$\begin{aligned} k \cdot b' \cdot a' = n \cdot b' \Rightarrow k \cdot a' = n \Rightarrow M = k \cdot b' \cdot a \Rightarrow (M) \subset (a \cdot b') \\ a \cdot b' = a' \cdot b \in (a) \cap (b) = (M),\ (a \cdot b') \subset (M) \\ (M) = (a \cdot b') = (a' \cdot b) = (a' \cdot b' \cdot d) \\ M = a' \cdot b' \cdot d \end{aligned}$$

Ejemplo

Calcular el mínimo común múltiplo de los números del ejemplo anterior.

$$\begin{aligned} a &= 126 \quad ; \quad b = 93 \quad ; \quad d = 3 \\ a' &= 42 \quad ; \quad b' = 31 \end{aligned}$$

$$M(126,93) = 42 \times 31 \times 3 = 3.906$$

3.13. EL CONJUNTO Q

3.131. Necesidad de ampliar Z

En el dominio de integridad de los enteros $[Z, +, \times]$ no siempre tiene solución la ecuación

$$a \cdot x = b \qquad [34]$$

Si $b \neq \dot{a}$, no existe ningún $x \in Z$ que satisfaga la igualdad establecida.

Con el fin de conseguir que la ecuación [34] tenga siempre solución, se crea un nuevo conjunto de números en el que la división siempre es posible.

El proceso consiste en simetrizar el dominio de integridad $[Z, +, \times]$, creando el cuerpo conmutativo $[Q, +, \times]$, siguiendo la técnica cuyo desarrollo en forma general se expuso en el número 2.72.

3.132. Creación del cuerpo $[Q, +, \times]$. Simetrización del dominio de integridad $[Z, +, \times]$

3.1321. *El semigrupo a simetrizar* $[Z, \times]$

Se dispone del anillo abeliano con elemento unidad, cancelativo (= sin divisores del cero), es decir, del dominio de integridad $[Z, +, \times]$; y en él, del semigrupo multiplicativo abeliano con elemento unidad $[Z, \times]$.

Se construye el cartesiano $Z \times Z^0$, en el que Z^0 representa el conjunto Z privado del cero.

Se establece la siguiente relación de equivalencia sobre $Z \times Z^0$:

$$\forall (a, b) \in Z \times Z^0,\ \forall (c, d) \in Z \times Z^0,\ (a, b) \equiv (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

El análisis de R la justifica como relación de equivalencia. (Realícese.)

Al actuar sobre $Z \times Z^0$, clasifica y parte a ese cartesiano en clases de equivalencia, formando el conjunto cociente

$$Q = Z \times Z^0/R = \left\{ \left\{ \frac{a_1}{b_1} \equiv \frac{a_2}{b_2} = \ldots \right\},\ \frac{c_1}{d_1} \equiv \frac{c_2}{d_2} = \ldots \right\} \ldots \Bigg\}$$

(Se han dispuesto los pares en la forma tradicional de fracción.)

Representantes canónicos: Se conviene en tomar como representante canónico de cada clase racional la única fracción irreducible de denominador positivo. En efecto, esto es posible siempre:

Sea $\left\{ \frac{a_1}{b_1} \equiv \frac{a_2}{b_2} \right\} \in Q.$

$$\frac{a_1}{a_2} = \frac{b_1}{b_2},\ d(a_1, a_2) = d(b_1, b_2) = 1,\ a_2 > 0,\ b_2 > 0.$$

Establecido lo que precede, justifiquemos que se trata de la misma fracción:

$$a_1 \cdot b_2 = b_1 \cdot a_2 \Rightarrow (a_2/b_2) \wedge (b_2/a_2);$$

luego

$$b_2 = \pm a_2.$$

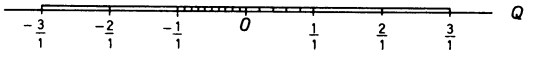
Finalmente, como

$$a_2 \in Z^+ \quad \text{y} \quad b_2 \in Z^+,$$

$$(a_2 = b_2) \wedge (a_1 = b_1)$$

Representación gráfica. La recta racional

Sobre la recta Q se dispone un punto 0, representante del racional $\{0\}$. A derecha y a izquierda se marcan puntos equidistantes, representativos de los racionales



$\left\{\frac{1}{1}\right\}$, $\left\{\frac{2}{1}\right\}$, $\left\{\frac{3}{1}\right\}$, $\cdots$ y de los racionales $\left\{\frac{-1}{1}\right\}$, $\left\{\frac{-2}{1}\right\}$, $\left\{\frac{-3}{1}\right\}$, $\cdots$ respectivamente.

Para representar cualquier racional $\left\{\frac{a}{n}\right\}$, se dividen en n partes iguale cada uno de los segmentos determinados antes y se toman a derecha $(+a)$ o a izquierda $(-a)$, a partes de las conseguidas.

De este modo, quedan representados en la recta los infinitos puntos racionales.

En cualquier segmento de la recta racional, por pequeño que sea, existen infinitos puntos racionales, como se demostrará luego. Sin embargo, son también «incontables» los puntos «que faltan» para «llenar» la recta: son los números reales irracionales. Se puede decir de un modo «plástico», entonces, que la recta racional está formada por infinitos puntos racionales e infinitos «agujeros» irracionales.

3.1322. *El cuerpo de fracciones del dominio de integridad Z*

A) La ley producto en Z es estable frente a la relación de equivalencia que define Q, a partir de $Z \times Z^0$. Se induce una ley multiplicación entre las clases de Q^0 que le estructura en forma de grupo*.

$$\forall\{a, b\} \in Q^0 \quad , \quad \forall\{c, d\} \in Q^0,$$
$$\{a, b\} \times \{c, d\} = \{a \cdot c,\ b \cdot d\}$$

B) Por lo que se refiere a la adición, a partir del grupo abeliano $[Z, +]$, se induce entre las clases de Q la siguiente operación:

$$\forall\{a, b\} \in Q \quad , \quad \forall\{c, d\} \in Q,$$
$$\{a, b\} + \{c, d\} = \{(a \cdot d + b \cdot c,\ b \cdot d)\}$$

Se ha de justificar ahora que $[Q, +]$ es un grupo abeliano.

---

* Adviértase que la multiplicación actúa sobre $Q^0 = Q - \{0\}$ y no sobre Q. Es necesario prescindir de la clase racional 0, para que, siendo inversibles todos los elementos, $[Q^0, \times]$ sea grupo.
Consúltese, si es necesario, el número 2.4322.

B-1) La adición establecida entre las clases de Q es uniforme por ser estable frente a la relación de equivalencia que creó Q a partir de $Z \times Z^0$. Basta, para probarlo, justificar que el resultado de operar dos clases racionales no depende de las fracciones escogidas como operandos. (Puede encontrarse la demostración en el número 2.722.)

B-2) Es inmediato probar que $[Q, +]$ goza de asociatividad.

B-3) Existencia de elemento neutro.
Basta operar, para justificar que

$$\forall \left\{\frac{a}{b}\right\} \in Q,\ \exists^* \left\{\frac{0}{m}\right\} \in Q / \left\{\frac{a}{b}\right\} + \left\{\frac{0}{m}\right\} = \left\{\frac{0}{m}\right\} + \left\{\frac{a}{b}\right\} = \left\{\frac{a}{b}\right\}$$

B-4) Elementos opuestos.

$$\forall \left\{\frac{a}{b}\right\} \in Q,\ \exists^* \left\{\frac{-a}{b}\right\} \in Q / \left\{\frac{a}{b}\right\} + \left\{\frac{-a}{b}\right\} = \left\{0\right\}$$

C) La multiplicación en Q es distributiva respecto de la adición. (Véase número 2.722.)

De este modo, ha quedado establecido el cuerpo de fracciones del anillo de integridad de los enteros $[Q, +, \times]$.

Siendo todo cuerpo anillo de integridad, todos los establecimientos hechos para el anillo de integridad de los enteros son válidos para el cuerpo de los racionales. Así, por ejemplo, recordemos el concepto de característica: siendo $x \in Q$ y $n \in Z^+$, expresamos el conjunto aditivo de n operandos así:

$$x + x + x + \ldots (n \text{ veces} = n \cdot x)$$

El menor n que hace $n \cdot x = 0$ es la característica del cuerpo. Inmediatamente se observa que Q no posee característica, pues no hay un $x \in Q / n \cdot x = 0,\ n \in Z^+$.

Ya quedó escrito que en este caso se dice que Q es un cuerpo de característica infinita.

3.133. El dominio de integridad *Z* sumergido en el cuerpo *Q*

1. Se establece la aplicación f entre el dominio de integridad Z y el cuerpo de sus fracciones Q, cuyo criterio es

$$[Z, +, \times] \xrightarrow{f} [Q, +, \times]$$
$$a \longrightarrow f(a) = \left\{\frac{a \cdot x}{x}\right\}, \quad \text{para } x \in Z^0$$

Que $\left\{\frac{a \cdot x}{x}\right\}$ es una clase racional, quedó justificado de modo general en el número 2.57.

2. La aplicación f, obviamente, es un homomorfismo inyectivo multiplicativo, es decir, un monomorfismo entre $[Z, \times]$ y $[Q^0, \times]$.
   Si se restringe el monomorfismo f al subconjunto de Q^0 formado por las imágenes de Z, aparece un monomorfismo epimórfico, o sea, un isomorfismo.
3. La aplicación f es un monomorfismo aditivo entre $[Z, +]$ y $[Q, +]$. Para justificarlo, veamos primero que es homomorfismo y, luego, que es inyectivo:

3.1)
$$\left\{\frac{a \cdot x}{x}\right\} + \left\{\frac{b \cdot y}{y}\right\} = \left\{\frac{a \cdot x \cdot y + x \cdot b \cdot y}{x \cdot y}\right\} =$$
$$= \left\{\frac{(a + b) \cdot x \cdot y}{x \cdot y}\right\} = \left\{\frac{c \cdot (x \cdot y)}{(x \cdot y)}\right\}$$

$$\forall a \in Z,\ \forall b \in Z,\ a + b = c,\ c \in Z;$$

es decir:

$$f(a) + f(b) = f(c)$$

3.2) Se comprueba ahora que cumple el teorema 2.563, que exige que el núcleo ha de ser unitario para que el homomorfismo sea inyectivo: $\ker(f) = \{0\}$.

Sea un $a \in \ker(f)$ y sea $\left\{\frac{0}{m}\right\} \in Q$ el neutro aditivo del cuerpo de fracciones. Entonces,

$$\left\{\frac{a \cdot x}{x}\right\} = \left\{\frac{0}{m}\right\} \Leftrightarrow a \cdot x \cdot m = x \cdot 0$$

Por ser Z de integridad, admite la simplificación (ley cancelativa)

$$a \cdot m = 0;$$

pero, siendo $m \neq 0$,

$$a = 0;$$

es decir:

$$\ker(f) = \{0\}, \qquad \text{c.q.d.}$$

Si se restringe el monomorfismo f al subconjunto de Q^0, formado por las imágenes de Z, se obtiene una f exhaustiva: un isomorfismo.

De este modo, se puede decir de alguna manera que el cuerpo creado ha captado al dominio que lo generó. A eso se refiere el vulgarismo $Z \subset Q$.

En realidad, lo que sucede es que se asimila el dominio de integridad Z al subconjunto de Q, imagen suya, en el isomorfismo que hemos venido estableciendo.

3.134. El cuerpo ordenado $[Q, +, \times, \leq]$

Recuérdese lo que se entiende por cono positivo de un grupo ordenado $[G, +, \leq]$

$$P^+ = \{x/(x \in G) \wedge (x \geq 0)\}$$

Con ello, se establece sobre Q la relación de orden

$$\alpha \in Q,\ \beta \in Q,\ \alpha \leq \beta \Leftrightarrow \beta - \alpha \in P^+ = Q^+ \cup \{0\}$$

Es fácil demostrar que la relación establecida es reflexiva, antisimétrica y transitiva, por lo que puede decirse que $[Q, \leq]$ es un orden amplio.

Además:

$$\forall \alpha,\ \beta \in Q \qquad (\alpha \leq \beta) \vee (\beta \leq \alpha).$$

En efecto:

$$\beta - \alpha \in P^+ \Rightarrow \alpha \leq \beta,$$

o bien

$$\beta - \alpha \in P^- \Rightarrow (\alpha - \beta) \in P^+ \Rightarrow \beta \leq \alpha$$

Se trata, pues, de un orden total.

Para decir que $[Q, +, \times, \leq]$ es un cuerpo totalmente ordenado, habrá de probarse ahora que, considerado como anillo, la estructura algebraica y la de orden son compatibles, en el sentido siguiente:

I. $\forall \gamma \in Q,\ \alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$
II. $\forall \gamma \in Q,\ (\alpha \leq \beta) \wedge (\gamma \geq 0) \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$

En efecto:

I. $\alpha \leq \beta \Rightarrow \beta - \alpha \in P^+ \Rightarrow \beta - \alpha = (\beta + \gamma) - (\alpha + \gamma) \in P^+ \Rightarrow \alpha + \gamma \leq \beta + \gamma$
II. $(\alpha \geq 0) \wedge (\beta \geq 0) \Rightarrow \alpha \cdot \beta \geq 0$

lo que implica que

$$(\alpha \leq \beta) \wedge (\gamma \geq 0) \Rightarrow (\beta - \alpha) \cdot \gamma \geq 0;$$

es decir:

$$\alpha \cdot \gamma \leq \beta \cdot \gamma.$$

Ya se puede asegurar que $[Q, +, \times, \leq]$ es un cuerpo totalmente ordenado.

Por otra parte, como el orden definido sobre el anillo Z es arquimediano, existe siempre un $c \in Z^+$, tal que $c \cdot \alpha > \beta$, para cualquier pareja de racionales estrictamente positivos α y β.

Finalmente, para terminar la cualificación del orden en Q, establezcamos el siguiente

TEOREMA. Todos los intervalos abiertos $(\alpha, \beta) \in Q$, $(\alpha < \beta)$, no son vacíos.

En efecto: dados dos racionales cualesquiera α y β, siempre se puede encontrar al menos un racional γ, tal que $\alpha < \gamma < \beta$.

Dando a γ el valor $\gamma = \dfrac{\alpha + \beta}{2}$, queda justificado el teorema.

A los órdenes en los que se satisface este teorema se les adjetiva «densos sobre sí mismos».

Resumiendo en una frase todos los resultados del análisis del orden racional que se ha venido realizando, se concluye:

> $[Q, +, \times, \leq]$ es un cuerpo totalmente ordenado, arquimediano y denso sobre sí mismo.

Cerrando el capítulo, se relacionan a continuación siete proposiciones referentes al orden racional. Las cinco primeras, comunes al anillo ordenado de los enteros, están demostradas, de forma general, en el número 2.74; las dos últimas, privativas de los cuerpos ordenados, también se han justificado ya en el número 2.743.

Proposición 1. $x, y \in Q \quad , \quad x \leq y \Rightarrow -y \leq -x.$

Proposición 2. Signando P^+ y P^- los conos positivo y negativo racionales, se verifica

$$P^+ \cap P^- = \{0\}$$

Proposición 3. $x, y \in Q,\ x \leq y \Leftrightarrow y - x \geq 0$; o sea: $y - x \in P^+$.

Proposición 4. $x, y \in Q,\ (x \geq 0) \wedge (y \geq 0) \Rightarrow x + y \geq 0.$

Proposición 5. $x, y \in Q,\ (x \geq 0) \wedge (y \geq 0) \Rightarrow x \cdot y \geq 0.$

Proposición 6. $x \in Q^+ \Rightarrow \dfrac{1}{x} \in Q^+$

$$x \in Q^- \Rightarrow \frac{1}{x} \in Q^-.$$

Proposición 7. $[(x, y \in Q^+) \vee (x, y \in Q^-)] \wedge (x \leq y) \Rightarrow \dfrac{1}{y} \leq \dfrac{1}{x}.$

3.14. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

3.140.

Demuéstrese en el conjunto de los cardinales $\mathfrak{C}$, que $a^m \times a^n = a^{m+n}$.

3.141.

Justifíquese que, siendo $a < b$, $\text{card}[a, b] = \aleph_1$.

3.142.

Demuéstrese que si $a, b \in \mathfrak{C}$, $a \leq b$, $\forall c \in \mathfrak{C}$, $a^c \leq b^c$.

3.143.

¿Es numerable el conjunto de los múltiplos de cinco? ¿Qué estructuras aditiva y multiplicativa tiene?

3.144.

Calcúlese el mayor entero que al dividir a 9.039 y a 4.352 produce en ambos casos de resto 9.

3.145.

Determínese el mayor entero que al dividir a 2.708 da de resto 17; y que al hacerlo a 2.000, produce de resto 11.

3.146.

Determínense los enteros x e y, sabiendo que $M(x, y) = 48.484$; $d(x, y) = 124$.

3.147.

Determínense los enteros que resuelven el sistema

$$\begin{aligned} x - y &= 240 \\ M(x, y) &= 1.260 \end{aligned}$$

3.148.

La adición de dos enteros es 371 y su M es 430 veces mayor que su d. Determínense.

3.149.

Determínese el menor valor de $y \in Z^+$ que satisface la congruencia

$$(9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10) \equiv y \ (730.$$

3.2

Circuitos

3.21. Algebra de interruptores

3.211. *Introducción*
3.212. *Establecimientos. Conexiones. Funciones de transmisión. Tablas de verificación*
3.213. *Circuitos compuestos*
3.214. *Interruptores complementarios*
3.215. *El álgebra de Boole de los circuitos. Algebra binaria*
3.216. *Simplificación de circuitos*
3.217. *Diseño de circuitos sencillos*

3.22. Sistema de numeración binaria

3.221. *Establecimientos. Bases*
3.222. *Adición binaria con interruptores*

3.2221. Sumadora intermedia
3.2222. Sumadora completa

3.223. *Diseños lógicos. Adición binaria mediante válvulas*

3.2231. Sumadora intermedia
3.2232. Sumadora completa

3.23. Aplicabilidad. Automatismos y destrezas

3.2

Algebra de circuitos

3.21. ALGEBRA DE INTERRUPTORES

3.211. Introducción

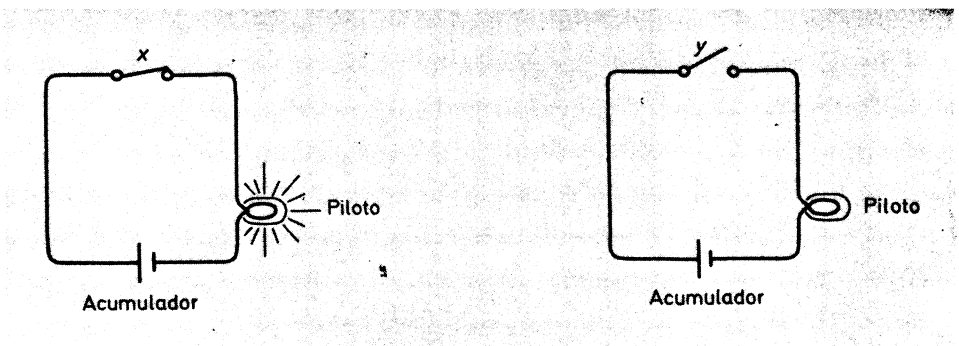
El gran auge de las comunicaciones telefónicas, por un lado, el gigantismo de la Cibernética, por otro, han exigido la matematización básica de estas ramas de la Ingeniería, a fin de poder abordar con éxito los complejos circuitos de interruptores mecánicos, electrónicos o electromecánicos a que dan lugar los diseños de las dos técnicas citadas.

Como corresponde a estas páginas de iniciación, se realiza un tratamiento de la cuestión elemental y esquemático. Así, siempre se considerarán interruptores simples e idealizados, en el sentido de que cierran o abren «del todo» el circuito; la corriente eléctrica implicada, salvo indicación en contrario, se entenderá continua y, consecuentemente, no existirán en nuestros desarrollos la reactancia inductiva ni la capacitancia; incluso, para nada se tendrá en cuenta la resistencia óhmica, al considerar el circuito absolutamente ideal.

Cerrando el capítulo, se expondrán los diseños lógicos de una sumadora intermedia y de una completa, mediante válvulas en lugar de interruptores. Sin entrar, de ningún modo, en la descripción «interna» de tales válvulas, entendemos, sin embargo, que la aplicación directa de las ideas de la Lógica, para la construcción de estos diseños, es sumamente ilustrativa en la etapa de iniciación en que nos movemos, resultando un tratamiento de la adición binaria bastante más sencillo y adecuado que el que se realiza previamente con los circuitos de interruptores.

3.212. Establecimientos. Conexiones. Funciones de transmisión. Tablas de verificación

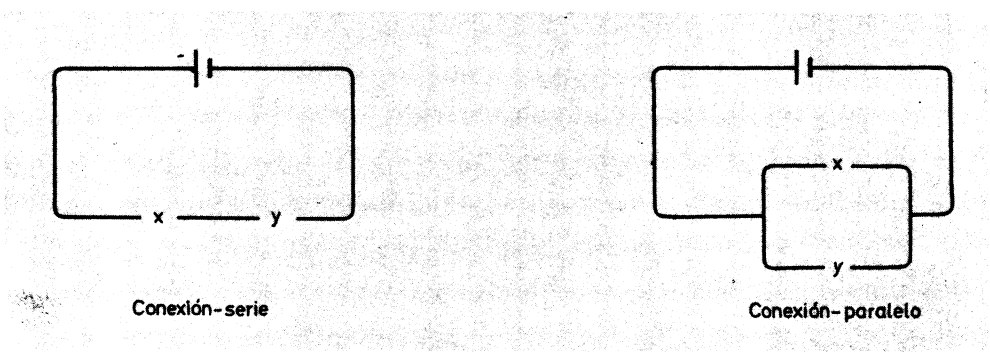
Se entiende por interruptor o conmutador todo aparato eléctrico susceptible de presentar dos estados de conducción. Se dirá que el conmutador está «abierto» si no deja pasar corriente; se entenderá que el interruptor está «cerrado» si permite el paso de toda la corriente. Todo, tal y como indica la figura adjunta.



Los interruptores se comportan como las variables del sistema y pueden tomar dos atributos excluyentes: abierto o cerrado. Convengamos en signar tales «valores» del siguiente modo: Si el interruptor x está cerrado y, por tanto, conduce, diremos que toma el valor 1; si por estar abierto no permite el paso de la corriente, le asignaremos el valor 0.

Los interruptores pueden conectarse entre sí de dos formas distintas: la conexión-serie y la conexión-paralelo.

La primera la denotaremos mediante el signo &; la segunda se representará con el símbolo ⫝.



$x \,\&\, y$ $\qquad\qquad$ $x \barwedge y$

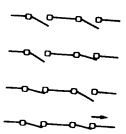
Con los convenios de escritura precedentes, llamaremos *función de transmisión* aquella que hace corresponder a los interruptores, la conexión que se establece entre ellos. Así, se escribe:

$$F_s = x \,\&\, y \quad ; \quad F_p = x \barwedge y$$

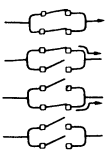
Los circuitos representados por las funciones de transmisión pueden conducir o no, en función de los posibles estados conductores de los interruptores que los integran. Se denomina *tabla de verificación* la descripción tabular de esos estados, junto con los de los interruptores que los provocan.

La atenta observación de cada uno de los circuitos y sus tablas de verificación es suficiente para comprender lo que se describe

Función de transmisión: serie

Circuito	x	y	$F_s = x \,\&\, y$
	1	1	1
	1	0	0
	0	1	0
	0	0	0

Función de transmisión: paralelo

Circuito	x	y	$F_p = x \,\barwedge\, y$
	1	1	1
	1	0	1
	0	1	1
	0	0	0

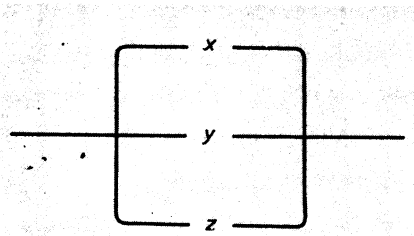
3.213. Circuitos compuestos

Los circuitos simples que hemos descrito, a su vez pueden conectarse entre sí, bien en serie, bien en paralelo, produciendo circuitos más complejos. Como la función de transmisión de la conexión-serie y la conexión-paralelo producen resultados 0 ó 1, la función de transmisión de un circuito complejo se forma por la composición de las funciones de transmisión de sus circuitos simples componentes; y su comportamiento algebraico es igual al descrito para interruptores. Así, siendo $F(x, y, \ldots)$ y $H(x, y, \ldots)$ dos funciones de transmisión, es posible su composición en serie o en paralelo, obteniéndose otras funciones de transmisión, cuyos comportamientos conductores se tabulan.

F	H	$F \,\&\, H$	$F \barwedge H$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

Ejemplo

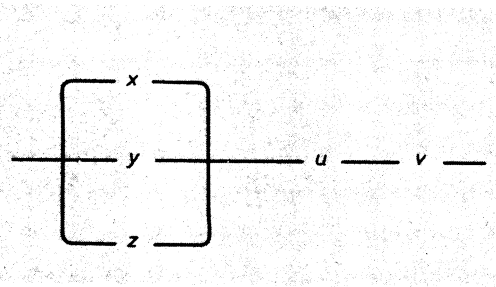
Sean los circuitos que se dibujan con las funciones de transmisión que los describen a su pie.

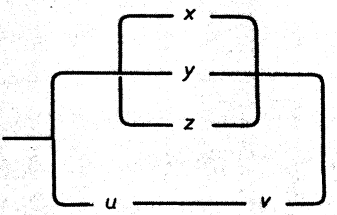


$F = x \barwedge y \barwedge z$

$H = u \,\&\, v$

A partir de ellos pueden montarse estos dos circuitos complejos



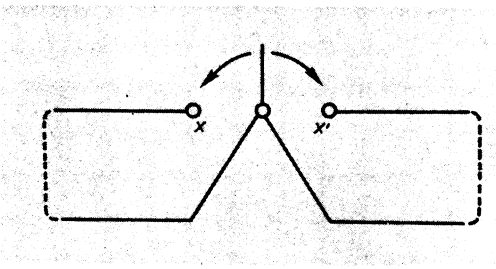


$F \,\&\, H = (x \barwedge y \barwedge z) \,\&\, (u \,\&\, v)$

$F \barwedge H = (x \barwedge y \barwedge z) \barwedge (u \,\&\, v)$

3.214. Interruptores complementarios

En un circuito puede suceder que, como intenta esquematizar la figura, existan dos interruptores tales que sus estados de conducción sean siempre opuestos; es decir, que si uno está cerrado, el otro se encuentra abierto, y viceversa.



A dos interruptores como los descritos, se les denomina interruptores *complementarios* y se conviene en denotarlos con la misma letra, para uno de ellos «limpia» y para el otro, «primada».

La tabla de verificación del montaje se induce de la propia definición de complementariedad, de modo que

x	x'
1	0
0	1

3.215. El álgebra de Boole de los circuitos. Algebra binaria

Sin duda se habrá venido observando la gran similitud del desarrollo precedente con el álgebra de proposiciones. En efecto, se trata aquí como allí de un álgebra booleana del todo-nada. Los valores de verdad de las proposiciones se corresponden con los estados conductores; la conjunción lógica es como la conexión-serie y la disyunción equivale a la conexión-paralelo, en el álgebra de circuitos. La negación proposicional está representada por los interruptores complementarios.

Además, así como allí dos proposiciones eran lógicamente equivalentes si sus tablas de verdad coincidían, aquí diremos que dos circuitos son equivalentes si sus funciones de transmisión presentan la misma tabla de verificación.

Con ello, se pasa a establecer la axiomática reticular del álgebra de Boole de los interruptores.

Teniendo en cuenta que todo circuito va asociado a su función de transmisión, utilizaremos el conjunto de éstas últimas, $\mathfrak{F}$, para formular sobre él los axiomas booleanos.

A_1) *Ley de absorción*

$$F \in \mathfrak{F},\ H \in \mathfrak{F},\ L \in \mathfrak{F}$$

$$F \,\text{đ}\, (F \,\&\, H) \equiv F \quad ; \quad F \,\&\, (F \,\text{đ}\, H) \equiv F$$

A_2) *Ley de idempotencia*

$$F \,\text{đ}\, F \equiv F \quad ; \quad F \,\&\, F \equiv F$$

A_3) *Ley de asociatividad*

$$F \,\text{đ}\, (H \,\text{đ}\, L) \equiv (F \,\text{đ}\, H) \,\text{đ}\, L \quad ; \quad F \,\&\, (H \,\&\, L) \equiv (F \,\&\, H) \,\&\, L$$

A_4) *Ley de conmutatividad*

$$F \,\text{đ}\, H \equiv H \,\text{đ}\, F \quad ; \quad F \,\&\, H \equiv H \,\&\, F$$

A_5) *Ley de complementariedad*

$$F \,\text{đ}\, F' \equiv 1 \quad , \quad F \,\&\, F' \equiv 0$$

$1 \in \mathfrak{F}$ es la conducción total (ausencia de interruptores),
$0 \in \mathfrak{F}$ es la transmisión nula (circuito fijo abierto).

A_6) *Ley de distributividad*

$$F \,\text{đ}\, (H \,\&\, L) \equiv (F \,\text{đ}\, H) \,\&\, (F \,\text{đ}\, L) \quad ; \quad F \,\&\, (H \,\text{đ}\, L) \equiv (F \,\&\, H) \,\text{đ}\, (F \,\&\, L)$$

Todas las leyes precedentes son fácilmente justificables mediante sus tablas de verificación.

Estas seis leyes establecidas dan al conjunto de las funciones de transmisión la estructura de retículo complementario distributivo, o lo que es igual, de álgebra de Boole.

A continuación se resaltan algunos de los teoremas básicos de esta álgebra, ordenados del mismo modo que se ha hecho en las cuatro ocasiones que en este libro se han desarrollado álgebras de Boole específicas (conjuntos, proposiciones, sucesos, circuitos).

Si se desea la justificación de algunos de ellos, basta traducir al lenguaje propio de circuitos las demostraciones que de todos, de modo general, se realizan en el número 2.14 del capítulo referente al álgebra de Boole abstracta. También el establecimiento de sus tablas de verificación justificaría la equivalencia de los circuitos.

T_7) *Ley de identidad* (cotas universales)

$$F \,\text{đ}\, 0 \equiv F \quad ; \quad F \,\&\, 1 \equiv F$$

T_8) *Ley de involución*

$$(F')' \equiv F$$

Consecuencia inmediata del teorema T_8 es el corolario

t_8) $$(0' \equiv 1) \wedge (1' \equiv 0)$$

T_9) *Ley de De Morgan*

$$(F \,\text{đ}\, H)' \equiv F' \,\&\, H' \quad ; \quad (F \,\&\, H)' \equiv F' \,\text{đ}\, H'$$

Algebra lógica o álgebra binaria. Suele recibir este nombre el álgebra booleana sobre dos elementos extremos excluyentes. Tal sucede con el {verdadero-falso} de las proposiciones y con el {abierto-cerrado} de los interruptores.

Abstrayendo a conceptos vacíos de todo contenido específico, sobre el conjunto $\{0, 1\}$ se crean tres operaciones, dos binarias y una unitaria, regidas por las tablas que se expresan y que obedecen a la axiomática y teoremática del álgebra de Boole establecida.

Adición lógica

+	0	1
0	0	1
1	1	1

Multiplicación lógica

×	0	1
0	0	0
1	0	1

Complementación lógica

~	0	1
	1	0

Al margen de los abundantes ejemplos que se han venido desarrollando de sistemas naturales obedientes a un álgebra binaria, aportemos ahora otro tan sugestivo como interesante: es del campo de la Genética.

De todos es conocido que en el cruce de dos caracteres genéticos, la generación filial segunda presenta el carácter dominante en un 75 por 100 y el recesivo en un 25 por 100. Pues bien, tal resultado responde totalmente a la adición lógica de caracteres.

Considérense dos ratas híbridas de la generación F_1, genotípicamente iguales. En su cruce se produce el acoplamiento de genes determinantes del color del pelo de los hijos, entre el dominante «negro» y el recesivo «blanco»; y todo sucede de acuerdo con el esquema booleano de la adición lógica. He aquí las tablas:

+	Blanco	Negro
Blanco		
Negro		

+	0	1
0	0	1
1	1	1

3.216. Simplificación de circuitos

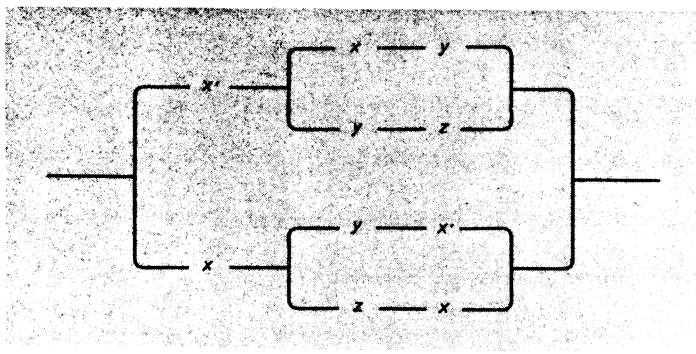
Dado un circuito de interruptores, es posible, usando la axiomática y teoremática del álgebra de Boole, simplificarle hasta formas más simples. Las fases del proceso son:

1.ª Dibujo del circuito-dato.
2.ª Establecimiento de su función de transmisión.
3.ª Simplificación booleana de la función de transmisión.
4.ª Dibujo del circuito de la función simplificada resultante.

El mejor modo de descripción es la realización de un ejemplo.

Ejemplo

Simplificar el circuito de la figura



La función de transmisión es:

$$F = [x' \,\&\, ((x \,\&\, y) \,\text{ɗ}\, (y \,\&\, z))] \,\text{ɗ}\, [x \,\&\, ((y \,\&\, x') \,\text{ɗ}\, (z \,\&\, x))]$$

Por conmutatividad:

$$F = [x' \,\&\, ((x \,\&\, y) \,\text{ɗ}\, (y \,\&\, z))] \,\text{ɗ}\, [x \,\&\, ((x' \,\&\, y) \,\text{ɗ}\, (x \,\&\, z))]$$

Por distributividad:

$$F = [x' \,\&\, (x \,\&\, y)] \,\text{ɗ}\, (x' \,\&\, (y \,\&\, z)) \,\text{ɗ}\, (x \,\&\, (x' \,\&\, y)) \,\text{ɗ}\, (x \,\&\, (x \,\&\, z))$$

Por asociatividad:

$$F = [(x' \,\&\, x) \,\&\, y] \,\text{ɗ}\, (x' \,\&\, y \,\&\, z) \,\text{ɗ}\, [(x \,\&\, x') \,\&\, y] \,\text{ɗ}\, [(x \,\&\, x) \,\&\, z]$$

Por complementación:

$$F = (0 \,\&\, y) \,\text{ɗ}\, (x' \,\&\, y \,\&\, z) \,\text{ɗ}\, (0 \,\&\, y) \,\text{ɗ}\, [(x \,\&\, x) \,\&\, z]$$

Por el teorema 1 del número 2.17 e idempotencia:

$$F = 0 \,\text{ɗ}\, (x' \,\&\, y \,\&\, z) \,\text{ɗ}\, 0 \,\text{ɗ}\, (x \,\&\, z)$$

Por identidad:

$$F = (x' \,\&\, y \,\&\, z) \,\text{ɗ}\, (x \,\&\, z)$$

Por distributividad:

$$F = [(x' \,\&\, y) \,\text{ɗ}\, x] \,\&\, z$$

Por distributividad:

$$F = [(x' \not\text{d}\, x) \,\&\, (y \not\text{d}\, x)] \,\&\, z$$

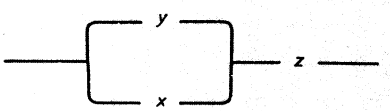
Por complementación:

$$F = [1 \,\&\, (y \not\text{d}\, x)] \,\&\, z$$

Por identidad:

$$F = (y \not\text{d}\, x) \,\&\, z$$

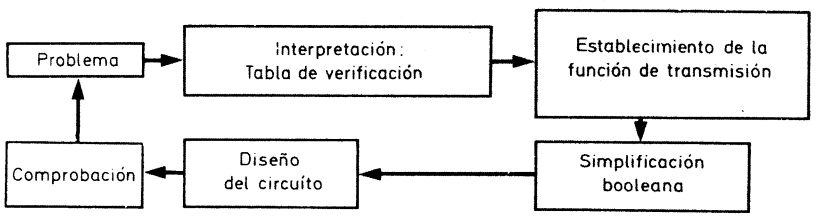
El circuito simplificado correspondiente es el que se dibuja.



3.217. Diseño de circuitos sencillos

En la práctica de la ingeniería el problema real que se presenta con más frecuencia es el inverso del hasta ahora descrito. Es decir, lo común es que se presente una situación o problema que exija unos determinados resultados y lo que ha de hacer el técnico es diseñar un circuito que actúe según las exigencias establecidas *a priori*.

Ante tal situación, conviene proceder según el siguiente esquema:



Como siempre que la ciencia «se hace técnica», el mejor modo de descripción es el desarrollo de ejemplos concretos.

Ejemplo 1

Se solicita de un instalador electricista que en las habitaciones de un hotel en construcción disponga un conmutador a la entrada y otro en la cabecera de la cama, de modo que ambos accionen la luz de la lámpara de noche, siendo capaces

cada uno de ellos de encenderla si está apagada, o de apagarla si está luciendo. ¿Cuál debe ser el circuito a diseñar?

Denotando los interruptores x e y, construyamos la tabla de verificación para la función de transmisión que exige el enunciado.

Supongamos, por ejemplo, que inicialmente ambos interruptores cerrados permiten que la lámpara esté encendida.

Situación	x	y	F
1.ª	1	1	1
2.ª	1	0	0
3.ª	0	0	1
4.ª	0	1	0

La segunda y cuarta situaciones no son de transmisión, no exigen nada y, por tanto, pueden ignorarse. La primera y la tercera son situaciones conductoras, de modo que la función de transmisión ha de ser tal que, produciéndose la primera «o» la tercera situación, en ambos casos se produzca conducción.

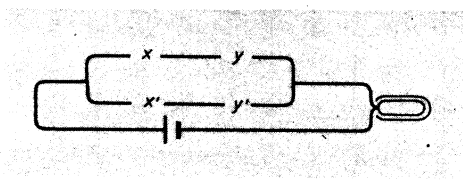
La primera exige que el interruptor x «y» el interruptor y estén cerrados para que haya conducción; la tercera, que el complementario de x esté cerrado «y» que el complementario del y, también.

Así, se establece la función

$$F = (x \,\&\, y) \,\text{d}\, (x' \,\&\, y'),$$

que obedece a la tabla de verificación planteada.

El circuito a que se refiere es suficientemente simple para no intentar su simplificación. Es el que se dibuja



Ejemplo 2

Dos matrimonios han de trasladarse desde un hotel a una fiesta usando un coche deportivo de dos plazas; pero ha de hacerse de tal manera que en ningún momento ninguna mujer esté sin su esposo en compañía del otro hombre. Los cuatro son capaces de conducir. ¿Cómo ha de llevarse a cabo el traslado?

Diséñese un circuito con cuatro interruptores, de modo que se encienda un piloto cuando se obtenga alguna combinación incorrecta.

Denotemos los matrimonios $A \circ\!\sim\!\circ\, a$ y $B \circ\!\sim\!\circ\, b$, y construyamos la tabla de verificación de las situaciones, signando 1 la localización en el hotel y 0 la presencia en la fiesta. De igual manera, escribimos 0 (¡atención!) para indicar combinaciones correctas y 1 para señalar las incorrectas:

Situaciones	*A*	*B*	*a*	*b*	*F*
1.ª	1	1	1	1	0
2.ª	1	0	1	1	1
3.ª	0	1	1	1	1
4.ª	0	0	1	1	0
5.ª	1	1	0	1	0
6.ª	1	0	0	1	1
7.ª	0	1	0	1	0
8.ª	0	0	0	1	0
9.ª	1	1	1	0	0
10.ª	1	0	1	0	0
11.ª	0	1	1	0	1
12.ª	0	0	1	0	0
13.ª	1	1	0	0	0
14.ª	1	0	0	0	1
15.ª	0	1	0	0	1
16.ª	0	0	0	0	0

Según la tabla, la función de transmisión representativa de todas las posiciones incorrectas es (sustituimos los signos & y ⊄ por los más cómodos, · y +, respectivamente):

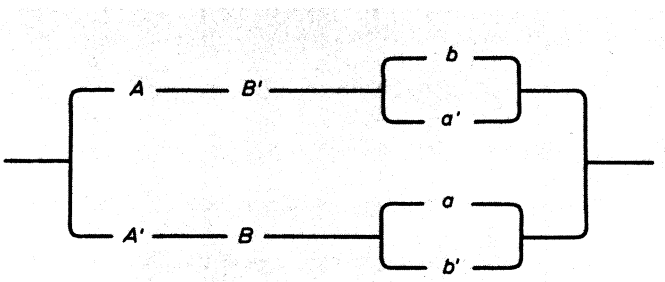
$$F = A \cdot B' \cdot a \cdot b + A' \cdot B \cdot a \cdot b + A \cdot B' \cdot a' \cdot b + A' \cdot B \cdot a \cdot b' + \\ + A \cdot B' \cdot a' \cdot b' + A' \cdot B \cdot a' \cdot b'$$

Se procede a su simplificación:

$$F = A \cdot B' \cdot [b \cdot (a + a') + a' \cdot b'] + A' \cdot B \cdot [a \cdot (b + b') + a' \cdot b']$$
$$F = A \cdot B' \cdot (b + a' \cdot b') + A' \cdot B \cdot (a + a' \cdot b')$$
$$F = A \cdot B' \cdot [(b + a') \cdot (b + b')] + A' \cdot B \cdot [(a + a') \cdot (a + b')]$$

$$\boxed{F = A \cdot B' \cdot (b + a') + A' \cdot B \cdot (a + b')}$$

Se construye el circuito en el que (compruébese) se encenderá el piloto cada vez que se produzca cualquiera de las situaciones inadmisibles.



Así, pues, las soluciones del problema son:

Hotel/Fiesta	$A-a$	$A-B$	$B-b$
Fiesta/Hotel	A	B	

Hotel/Fiesta	$a-b$	$A-B$	$A-a$
Fiesta/Hotel	a	A	

Hotel/Fiesta	$a-b$	$A-B$	$B-b$
Fiesta/Hotel	b	B	

Hotel/Fiesta	$B-b$	$A-B$	$A-a$
Fiesta/Hotel	B	A	

3.22. SISTEMA DE NUMERACION BINARIA

3.221. Establecimientos. Bases

Desde la escuela se sabe que es posible establecer diversas expresiones numéricas de una misma cantidad, según la base de numeración que se escoja.

Se demuestra fácilmente el teorema fundamental de la numeración, que dicta:

Todo número A puede descomponerse, de manera única, en la forma polinómica

$$A = a \cdot m^0 + b \cdot m^1 + c \cdot m^2 + \cdots + p \cdot m^n$$

$$a, b, c, \ldots, p \in N \cup \{0\}$$
$$a, b, c, \ldots, p \in s(m)$$
$$m \in N \quad , \quad m > 1$$

Los símbolos significan que la base ha de ser un natural mayor que uno y que las cifras a, b, c, ..., p, han de ser ceros o naturales menores que la base m.

Ejemplo 1

El número 79 301, escrito en base 10, se expresa polinómicamente así:

$$79\,301_{(10} = 1 \cdot 10^0 + 0 \cdot 10^1 + 3 \cdot 10^2 + 9 \cdot 10^3 + 7 \cdot 10^4$$

Ejemplo 2

El número escrito en base 5, 3 401 es igual a la expresión polinómica

$$3\,401_{(5} = 1 \cdot 5^0 + 0 \cdot 5^1 + 4 \cdot 5^2 + 3 \cdot 5^3$$

Para pasar un número expresado en base m a su expresión en base n, primero, mediante su desarrollo polinómico, se alcanza su expresión en base 10 y, luego, por divisiones sucesivas, se consigue su expresión en base n.

Claro es que, si el dato es un número en base 10, basta el último paso indicado para obtener su expresión en la base deseada. Todo como se hace en el siguiente ejemplo.

Ejemplo

Obtener la expresión en base 3, del número $14_{(5}$.

$$14_{(5} = 4 \cdot 5^0 + 1 \cdot 5^1 = 9_{(10}$$

$$\begin{array}{r|l} 9 & 3 \\ \hline 0 & 3 \quad \begin{array}{|l} 3 \\ \hline 1 \end{array} \\ & 0 \end{array} \qquad 14_{(5} = 9_{(10} = 100_{(3}$$

De todos los sistemas de numeración no decimales, el de mayor importancia, sin duda, es el sistema binario, que es el que tiene de base 2. En él, los únicos guarismos a utilizar son el 0 y el 1, lo que supone expresiones muy largas, aun para cantidades pequeñas. Eso, que sería una dificultad grande para cálculo directo, es precisamente su ventaja como base de los computadores electrónicos. Efectivamente, éstas máquinas, obedientes al álgebra binaria booleana, son capaces de operar en base 2.

Recordemos las tablas de adición y multiplicación en base 2:

+	0	1
0	0	1
1	1	10

×	0	1
0	0	0
1	0	1

Obsérvese que la única diferencia con las operaciones lógicas binarias es que $1 + 1 = 10$, mientras que en la adición lógica se establecía que $1 + 1 = 1$.

3.222. Adición binaria con interruptores

3.2221. *Sumadora intermedia*

Se denomina así una máquina capaz de sumar dos dígitos binarios; o sea, capaz de realizar cualquiera de estas cuatro sumas:

$$\begin{array}{r} 0 \\ 0 \\ \hline 00 \end{array} + \begin{array}{r} 0 \\ 1 \\ \hline 01 \end{array} + \begin{array}{r} 1 \\ 0 \\ \hline 01 \end{array} + \begin{array}{r} 1 \\ 1 \\ \hline 10 \end{array} +$$

Para diseñarla, establezcamos una tabla de verificación con los sumandos y los totales

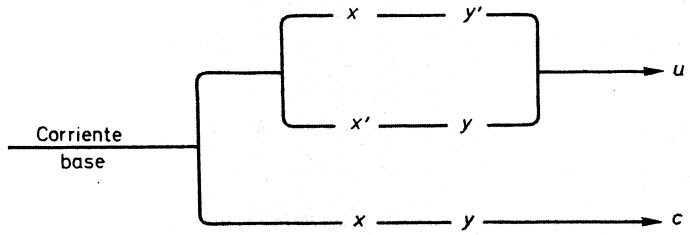
Primer sumando x	Segundo sumando y	Suma c	u
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Es elemental construir las dos funciones booleanas que producen el resultado c y el resultado u; son éstas:

$$c = x \cdot y$$
$$u = x \cdot y' + x' \cdot y$$

(A partir de ahora, se simbolizarán la conexión-serie y la conexión-paralelo por los signos respectivos · y +.)

El circuito, pues, de una sumadora intermedia «aislada»* es el que se dibuja:



3.2222. *Sumadora completa*

Recibe este nombre una máquina capaz de sumar tres dígitos binarios: un resultado que «se lleva» de la posible unidad anterior y dos nuevos sumandos.

Su tabla de verificación es:

«Se lleva» z	Primer sumando x	Segundo sumando y	Suma c	u
0	0	0	0	0
1	0	0	0	1
0	0	1	0	1
1	0	1	1	0
0	1	0	0	1
1	1	0	1	0
0	1	1	1	0
1	1	1	1	1

* Cáigase en la cuenta de que, más adelante, cuando haya que integrar esta sumadora intermedia con sumadoras completas, será necesario adosarle un circuito complementario del c, a fin de suministrar la señal necesaria a la siguiente unidad.

Las funciones que dan c y u son:

$$c = x' \cdot y \cdot z + x \cdot y' \cdot z + x \cdot y \cdot z' + x \cdot y \cdot z \qquad [1]$$

$$u = x' \cdot y' \cdot z + x' \cdot y \cdot z' + x \cdot y' \cdot z' + x \cdot y \cdot z \qquad [2]$$

Intentando la mayor claridad didáctica, nada se ha dicho aún de la naturaleza de las variables booleanas escritas; pero, ahora, antes de iniciar la simplificación, se hacen necesarias algunas puntualizaciones:

a) las representadas x e y, en efecto, pueden ser interruptores y funcionar como tales;

b) la denotada z no es interruptor, sino que es una señal de intensidad o potencial suministrada por la unidad previa de adición. No se trata, entonces, de un interruptor;

c) tanto en la función de las unidades como en la c, han aparecido símbolos z', que resultan ser las «señales complementarias» de las z.

Como la señal z procede del resultado c de la unidad anterior de adición, para suministrar la señal complementaria z', basta construir los circuitos complementarios de los c.

Cuidando de no tocar a z y z', la simplificación booleana de la función [1] arroja la expresión

$$c = z \cdot (x + y) + z' \cdot (x \cdot y) \qquad [3]$$

Del mismo modo, se consigue para [2] la función más simplificada

$$u = z' \cdot (x' \cdot y + x \cdot y') + z \cdot (x' \cdot y' + x \cdot y) \qquad [4]$$

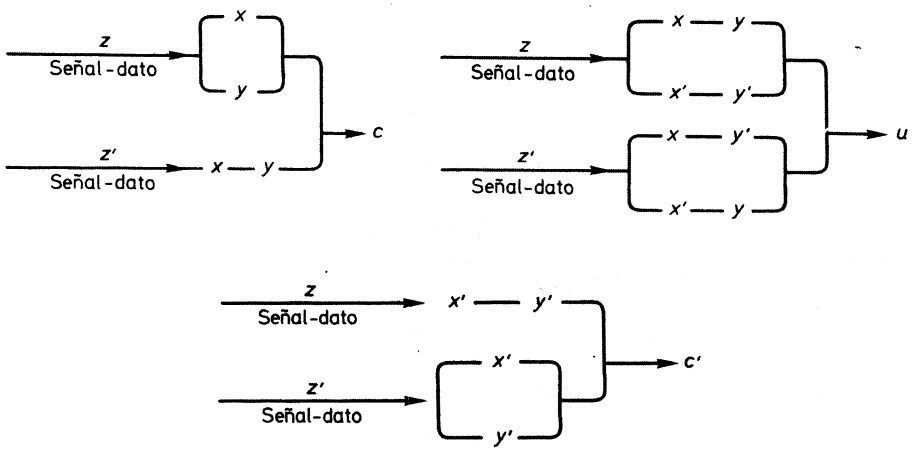
Por lo que se refiere al circuito complementario del c (preparando la señal z para la próxima unidad sumatoria), basta aplicar la ley de De Morgan a [3], para obtener, tras simplificar,

$$c' = z' \cdot (x' + y') + x' \cdot y';$$

y teniendo en cuenta que $z + z' = 1$, se «multiplica» el término $x' \cdot y'$ por $z + z'$ y, simplificando la expresión resultante, se obtiene finalmente para el circuito complementario la función

$$c' = z' \cdot (x' + y') + z \cdot (x' \cdot y') \qquad [5]$$

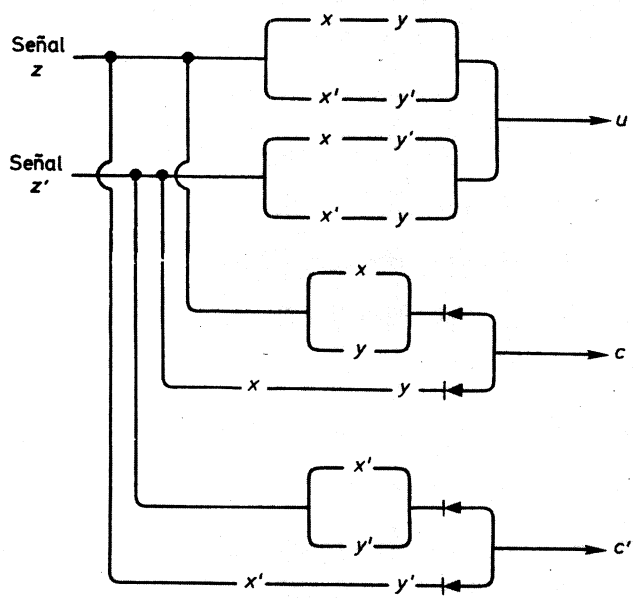
Los circuitos correspondientes a las funciones [3], [4] y [5] serían:



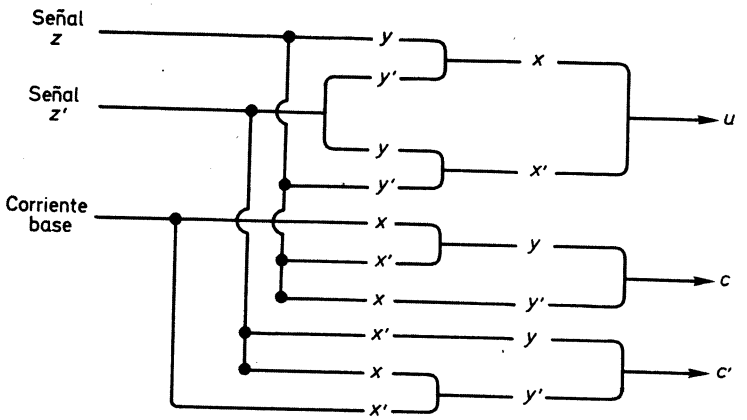
Antes de un montaje conjunto, todavía ha de atenderse a solventar una dificultad de tipo técnico. Tanto en el circuito c como en su complementario, en el caso en que estén cerrados los interruptores x e y ($x = 1$; $y = 1$) en el circuito c o abiertos en el c' ($x = 0$; $y = 0$), aparecen unas corrientes de z a z', cerradas sobre sí mismas.

Dos son los modos de resolver esta cuestión: o bien, intercalando adecuadamente interruptores monodireccionales (que sólo dejan pasar la corriente en un sentido, como pueden ser los diodos), o bien diseñar un nuevo circuito con corriente-base en cada paso que es el segundo que se dibuja.

Sumadora completa de interruptores con diodos



Sumadora completa de interruptores convencionales

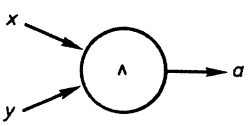


3.223. Diseños lógicos. Adición binaria mediante válvulas

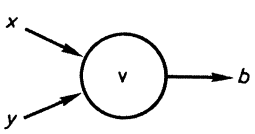
Un diseño más adaptado a los circuitos de las calculadoras en uso es el que se puede realizar, en lugar de con interruptores, con válvulas electrónicas* cuyo funcionamiento responde a las leyes booleanas del álgebra proposicional.

Así, disponemos de dos denominadas «válvula *y*» y «válvula *o*», que admiten dos datos y suministran una salida, de acuerdo con las tablas lógicas de su nombre. Además, se tiene la llamada «unidad de negación» cuyo funcionamiento, admitiendo un dato y dando un resultado, es acorde con la tabla veritativa de la negación lógica.

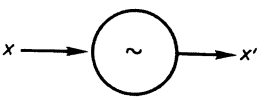
Los esquemas que siguen obedecen a las tablas que se adjuntan



Datos		Resultado
x	*y*	*a*
1	1	1
1	0	0
0	1	0
0	0	0



Datos		Resultado
x	*y*	*b*
1	1	1
1	0	1
0	1	1
0	0	0



Datos	Resultado
x	*x'*
1	0
0	1

* Para su descripción pueden consultarse las obras *We built our own computers*. «S. M. P. Handbook». Cambridge University Press, 1966. CALDWELL: *Switching circuits and logical designg*. Wiley, 1965.

3.2231. *Sumadora intermedia*

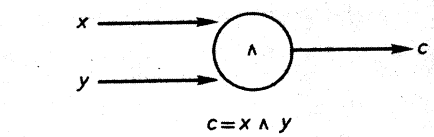
Como queda establecido en 3.222, las funciones booleanas que definen una sumadora intermedia son

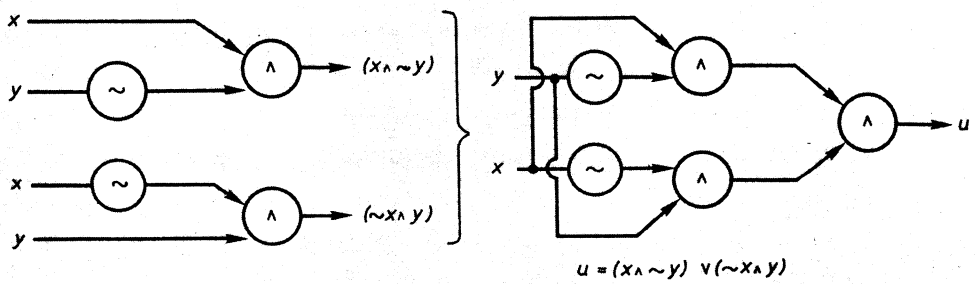
$$c = x \cdot y$$
$$u = x \cdot y' + x' \cdot y$$

referibles a la adición binaria

$$\begin{array}{r} x \\ y \; + \\ \hline c\; u \end{array}$$

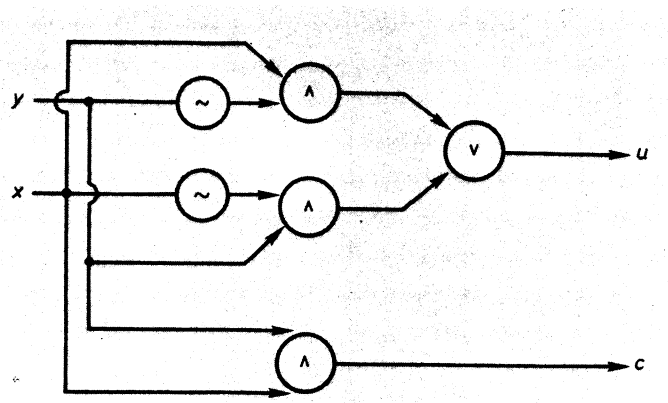
Entendiendo que lo que allí eran conexión-serie y conexión-paralelo aquí equivalen a la conjunción y disyunción lógicas, modelos de comportamiento de las «válvula *y*» y la «válvula *o*»; advirtiendo que las letras significaban interruptores abiertos o cerrados y aquí denotan presencia o ausencia de una señal (potencial); y comprendiendo finalmente que al disponer de una unidad de negación no es necesario montar circuitos para c', el diseño de una sumadora intermedia está formado por los siguientes circuitos de válvulas que —compruébense— satisfacen las funciones lógicas que se escriben a sus pies.



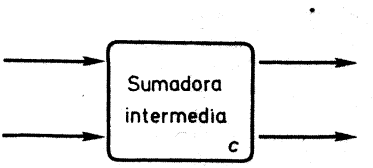


Finalmente, se integran los circuitos de las unidades *u* y del resultado «que se lleva», *c*, en un solo montaje.

Sumadora intermedia



Siendo la sumadora intermedia una unidad de montaje en diseños más complicados, construidos a base de multitud de ellas, se acostumbra a simbolizarla mediante el siguiente esquema:



3.2232. *Sumadora completa*

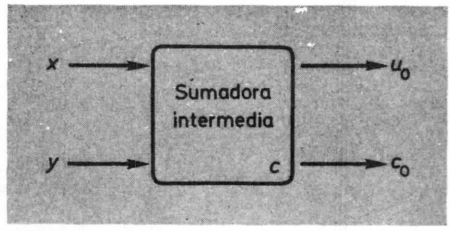
Se pretende ahora conseguir un diseño lógico de válvulas que sea capaz de sumar tres dígitos binarios

$$\begin{array}{r} x \\ y + \\ z \\ \hline c_2 u_1 \end{array}$$

Abordamos su construcción en tres fases.

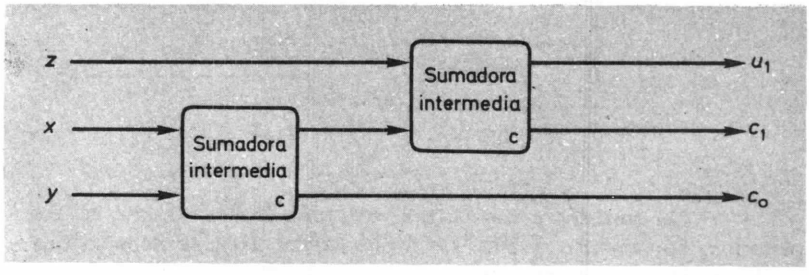
Primera fase. Una sumadora intermedia toma los datos x e y y los suma, produciendo una cifra de unidades u_0 y una cifra que «se lleva», c_0.

$$\begin{array}{r} x \\ y \\ \hline c_0 u_0 \end{array} +$$



Segunda fase. Una segunda sumadora intermedia se encarga de sumar las unidades u_0, suministradas por la primera, con el tercer sumando z, suministrando una cifra de unidades u_1 y una cifra que «se lleva» c_1

$$\begin{array}{r} u_0 \\ z \\ \hline c_1 u_1 \end{array} +$$



Tercera fase. Han de integrarse en la suma total los dos resultados que «se llevan», c_0 y c_1, de las dos sumadoras intermedias. Para ello, obsérvese que en cualquier caso, nunca es $c_0 = c_1 = 1$.

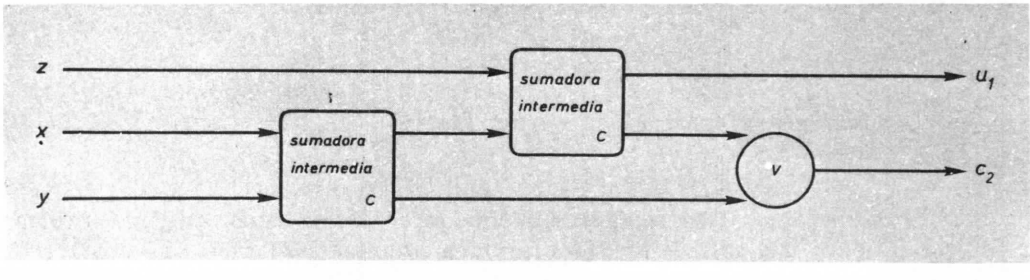
He aquí las ocho adiciones posibles y los valores que en cada una de ellas toman los parciales c_0 y c_1.

$1+1+1$	$1+1+0$	$1+0+1$	$0+1+1$	$0+0+1$	$0+1+0$	$1+0+0$	$0+0+0$
$c_0 = 1$	$c_0 = 1$	$c_0 = 0$	$c_0 = 0$	$c_0 = 0$	$c_0 = 0$	$c_0 = 0$	$c_0 = 0$
$c_1 = 0$	$c_1 = 0$	$c_1 = 1$	$c_1 = 1$	$c_1 = 0$	$c_1 = 0$	$c_1 = 0$	$c_1 = 0$

Entonces, una «válvula *o*» es capaz de integrar ambos resultados que «se llevan», produciendo su adición en todos los casos.

Según ello, el diseño total de una sumadora completa con válvulas es:

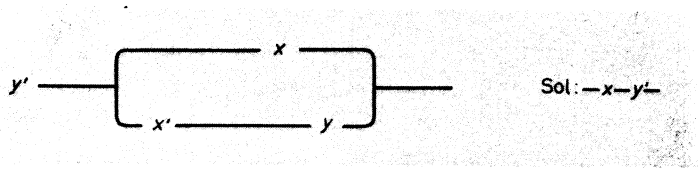
Sumadora completa



3.23. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

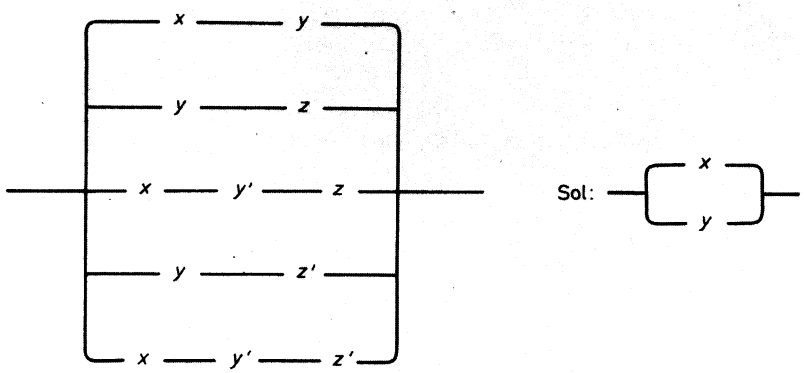
3.230.

Simplifíquese, mediante las leyes del álgebra de Boole, el circuito que se dibuja, estableciendo previamente su función de transmisión.



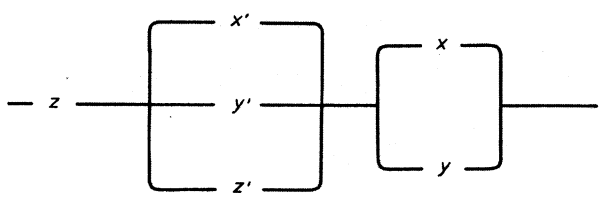
3.231.

Simplifíquese mediante las leyes del álgebra de Boole el siguiente circuito, estableciendo previamente su correspondiente función de transmisión.



3.232.

Establézcase la tabla de verificación del circuito



3.233.

Una lámpara de un garaje se desea que esté accionada desde el propio garaje y también desde el vestíbulo de la vivienda, de modo que cualquiera de los dos conmutadores sirva para cambiar el estado de la lámpara: apagarla, si está encendida, o encenderla, si está apagada. Diséñese el circuito correspondiente.

3.234.

Diséñese un circuito de interruptores capaz de detectar el mayor de todo par de dígitos.

3.235.

El sistema electrónico para la apertura de la bóveda de un banco implica a tres personas diferentes, con sus mandos correspondientes. Sólo se puede franquear si los tres controles son positivos, no abriéndose si uno cualquiera de los mandos envía señal negativa. Diséñese el circuito de interruptores correspondiente.

3.236.

Muéstrese que el número $13\,542_{(n}$ es múltiplo del $122_{(n}$, $\forall n > 5$. Determínese también su cociente.

3.237.

Determínese a, b, c y d, sabiendo que $0{,}8125 = 0{,}abcd_{(2}$.

3.238.

Usando una sumadora intermedia y dos completas, diséñese un circuito lógico que sea capaz de sumar dos números binarios de tres dígitos.

3.239.

Diséñese una multiplicadora para dos números binarios de dos dígitos.

3.3

Sucesos aleatorios

3.31. Introducción

3.32. Experiencia o prueba. Sucesos elementales. Espacio muestral

3.33. Sucesos compuestos. Suceso seguro

3.34. Conjunto-potencia de un espacio muestral, *H*

3.35. Orden e igualdad en el conjunto *P(H)*

3.351. *Inclusión de sucesos*
3.352. *Igualdad de sucesos*

3.36. Operaciones con sucesos

3.361. *Complementación. Sucesos contrarios. Suceso imposible*
3.362. *Unión*
3.363. *Intersección. Sucesos incompatibles*

3.37. Sistema completo de sucesos

3.38. Leyes del álgebra de sucesos. El álgebra de Boole de los sucesos estocásticos

3.39. Aplicabilidad. Automatismos y destrezas

3.3

Sucesos aleatorios

3.31. INTRODUCCION

Durante mucho tiempo fue doctrina común que el objeto de la ciencia, el «hecho científico» era todo aquello que podía encuadrarse dentro de una fenomenología determinista; es decir, sólo se podía aplicar el método científico a aquellos experimentos cuyos resultados eran los mismos, si las condiciones de ejecución eran iguales.

Superado este concepto, hoy el objeto de la ciencia es tanto los sucesos de la fenomenología determinista, como los hechos, no predecibles, de una fenomenología aleatoria, estocástica o de azar. Más aún: puede que esta última parcela, de extraordinaria importancia, no sea más que el salto enorme de haber conseguido descubrir y contemplar con «lupa más fina» lo que de aleatorio hay en los microhechos de la macrofenomenología determinista. Quedan muy lejos los conceptos del «electrón-bola», por ejemplo, y el del encorsetamiento copernicano de las estructuras electrónicas; hoy, la ley del azar, las funciones de probabilidad, el postulado de incertidumbre, son otros tantos hitos científicos de una ciencia, de una Matemática de la aleatoriedad.

Si se realiza la *experiencia* de añadir sodio sobre agua, tantas cuantas veces se haga la *prueba*, se producirá el mismo *suceso*: una violenta reacción genera gas hidrógeno y compone sosa cáustica. Se trata de un fenómeno determinista: el resultado de la experiencia es siempre el mismo suceso, y, por tanto, predecible.

Es bien conocido que la pareja 23 de cromosomas de la especie humana, en el hombre está formada por los distintos (X, Y) y en la mujer lo constituyen los iguales (X, X). Genéticamente, el sexo del hijo viene determinado porque el acoplamiento cromosómico produzca pares (X, X) o (X, Y). Resulta entonces que la prueba o experiencia de la fecundación natural produce un suceso cuyo resultado no es

predecible, por lo que se refiere al sexo del hijo; el azar interviene en el acoplamiento cromosómico, y todavía les es dado a los hombres la gracia de la incertidumbre, cuando esperan sus hijos. He aquí un fenómeno aleatorio.

3.32. EXPERIENCIA O PRUEBA. SUCESOS ELEMENTALES. ESPACIO MUESTRAL

Para describir —que no definir— el concepto *suceso*, tal vez sea bueno contemplar algunos sinónimos suyos: hecho, sucedido ... Se advierte que se trata de sustantivos derivados claramente de una forma verbal pasiva, o sea, pasada. Todo ello sugiere que un suceso, para que exista, ha de venir precedido de una determinada ejecución (real o fingida). En efecto: un *suceso* se presenta siempre como resultado de una *experiencia* o *prueba*.

Resulta así que, fijada una determinada experiencia, asociado a ella, aparece un conjunto de sucesos posibles, excluyentes entre sí, cada uno de los cuales recibe el nombre de *suceso elemental*; y el conjunto de sucesos elementales se denomina *espacio muestral*.

Ejemplo 1

Sea la experiencia aleatoria «Tirar un dado sobre la mesa y leer su cara superior en reposo».

Los sucesos elementales que la experiencia puede producir son seis: que salga y se lea el 1, el 2, el 3, el 4, el 5, el 6, de modo que el espacio muestral es el conjunto

$$H = \{h_1,\ h_2,\ h_3,\ h_4,\ h_5,\ h_6\}$$

3.33. SUCESOS COMPUESTOS. SUCESO SEGURO

Se denomina suceso compuesto (suceso, en general) a todo subconjunto $A \subset H$, del espacio muestral; y recibe el nombre de *suceso seguro* al suceso representado por el espacio muestral, completo.

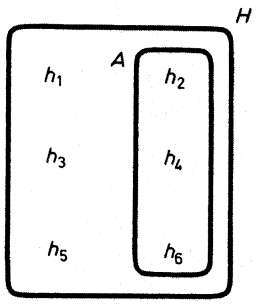
En esta línea de establecimientos, se puede definir ahora el concepto de suceso elemental como cualquier subconjunto unitario del espacio muestral.

Ejemplo 2

Sobre la misma experiencia del ejemplo anterior, analicemos en qué consiste el suceso A = «que salga y se lea un número múltiplo de 2».

Es claro que este suceso compuesto se verifica si sale y se lee 2, 4 ó 6, de modo que

$$A = \{h_2,\ h_4,\ h_6\}$$



Y ¿cuál es el suceso descrito de este modo: «que salga y se lea un número menor que 7»?

Evidentemente, se trata del suceso seguro, representado por el espacio muestral.

3.34. CONJUNTO-POTENCIA DE UN ESPACIO MUESTRAL, *H*

Se establece un espacio muestral $H = \{h_1, h_2, h_3\}$, de tres sucesos elementales, con el fin de no hacer farragosa la exposición.

El conjunto-potencia $P(H)$ es

$$P(H) = \{\phi, \{h_1\}, \{h_2\}, \{h_3\}, \{h_1, h_2\}, \{h_1, h_3\}, \{h_2, h_3\}, H\}$$

Sus $2^3 = 8$ elementos-conjunto son todos los sucesos a considerar (simples o compuestos), a partir de la experiencia generadora.

¿Qué representa el ϕ?, ¿qué suceso es? Es el *suceso imposible*, que ha de considerarse, para salvar la consistencia del álgebra de sucesos: se trata del suceso «pensado» que no se produce en la categoría de pruebas, generadora del sistema.

Un poco más adelante, al tratar la complementación, el suceso imposible nacerá desde otro punto de vista.

Ejemplo-Ejercicio 3

Sea la categoría de pruebas del ejemplo 1. Una forma de describir el suceso imposible sería

$$\phi = \text{«que salga y se lea 9»}.$$

Otro modo de describir el mismo suceso podría ser

$$\phi = \text{«que salga y se lea un múltiplo de 11»}.$$

¿Cuál es el suceso $\{h_1, h_3\}$?
¿Qué subconjunto describe el suceso «sacar múltiplo de 3»?
¿Y cuál el «obtener un número menor que 4»?

3.35. ORDEN E IGUALDAD EN EL CONJUNTO $P(H)$

3.351. Inclusión de sucesos

Sean A y B dos sucesos pertenecientes a la misma categoría de pruebas; de modo que, siendo H el espacio muestral, A y B son subconjuntos de H y, por tanto, elementos de $P(H)$:

$$\begin{array}{ll} A \subset H & B \subset H \\ A \in P(H) & B \in P(H) \end{array}$$

Se dice que A está incluido en B —denotado $A \subset B$— si el hecho de verificarse A implica que se realiza B.

Ejemplo 4

Sea la categoría de pruebas «extraer y leer una carta de una baraja de 52 naipes». Digamos que el suceso K es «conseguir un rey» y el F, «obtener una figura».

Es claro que $K \subset F$, puesto que, siempre que se consiga un rey, se ha obtenido una figura.

La inclusión de sucesos es una relación de orden $P(H)$, puesto que es reflexiva, antisimétrica y transitiva. En efecto, los planteamientos que siguen son inmediatos.

Reflexiva	$A \subset A,\ \forall A \in P(H)$
Antisimétrica	$(A \subset B) \wedge (B \subset A) \Leftrightarrow A \equiv B$
Transitiva	$(A \subset B) \wedge (B \subset C) \Rightarrow A \subset C$

El orden $(P(H), \subset)$ es un orden amplio parcial. Amplio, por ser reflexivo; parcial, pues dados dos cualesquiera sucesos A y B de $P(H)$, no siempre se puede establecer que $A \subset B$ o que $B \subset A$.

Ejemplo 5

Sea la categoría de pruebas del ejemplo anterior. Los sucesos A = «conseguir corazones» y B = «obtener un as» son dos sucesos que no se incluyen: ni el hecho de haber conseguido un as implica haber obtenido corazones, ni, si se ha verificado «corazones», se puede asegurar que se haya obtenido un as.

Dos sucesos A y B de los que no se puede escribir que $A \subset B$ o que $B \subset A$, se dice que son *sucesos no comparables*.

3.352. Igualdad de sucesos

Se establecen dos sucesos A y B de la misma categoría de pruebas H. Si sucede que A está incluido en B y B lo está en A, entonces A y B son dos sucesos iguales. O sea,

$$\left.\begin{matrix} A \subset B \\ B \subset A \end{matrix}\right\} \Leftrightarrow A \equiv B$$

Ejemplo 6

En una urna hay bolas blancas y otras coloreadas de azul, rojo o verde. En la categoría de pruebas «extraer una bola y constatar su color», se consideran los sucesos A = «extraer bola coloreada» y el suceso B = «conseguir una bola azul, roja o verde».

Siempre que se verifique A lo hace B; y siempre que suceda B, se ha conseguido bola coloreada, o sea, se ha llevado a cabo A. Quiere decirse que el suceso A está incluido en el B y que el B está incluido en el A. En fin, se trata del mismo suceso.

La igualdad de sucesos es una relación de equivalencia en $P(H)$, puesto que es reflexiva, simétrica y transitiva. La justificación es trivial.

Reflexiva	$A \equiv A, \ \forall A \in P(H)$
Simétrica	$A \equiv B \Leftrightarrow B \equiv A$
Transitiva	$\left.\begin{matrix} A \equiv B \\ B \equiv C \end{matrix}\right\} \Rightarrow A \equiv C$

3.36. OPERACIONES CON SUCESOS

3.361. Complementación. Sucesos contrarios. Suceso imposible

Considérese la categoría de pruebas que da lugar al espacio muestral H, formado por n sucesos elementales.

$$H = \{h_1, h_2, \ldots, h_n\}$$

Sea un suceso $A \subset H$. Se denomina *suceso contrario* del A —y se denota $\bar{A}$— al suceso que se verifica si, y sólo si, no lo hace A.

Entendamos que el suceso A está formado por los j elementales

$$A = \{h_1, h_2, \ldots, h_j\}.$$

Según la definición, el suceso contrario $\bar{A}$ habrá de estar constituido por los n-j sucesos elementales que completan el espacio muestral H, de modo que

$$\bar{A} = \{h_{j+1}, \ldots, h_n\}$$

Ejemplo 7

El suceso A es «conseguir un número mayor o igual que 4, al tirar un dado sobre una mesa». Será, pues,

$$A = \{h_4,\ h_5,\ h_6\}.$$

El suceso contrario $\bar{A}$ se verificará si no lo hace A, por tanto, el subconjunto representativo suyo es

$$\bar{A} = \{h_1,\ h_2,\ h_3\}.$$

Dos descripciones verbales de $\bar{A}$ pueden ser:

«No conseguir un número mayor o igual que 4»;
«Obtener un número menor que 4».

Se denomina *complementación* de sucesos la operación unitaria que produce como resultado el contrario del suceso operado.

Suceso imposible, denotado ϕ, es el contrario del suceso seguro, H.

$$\bar{H} = \phi$$

Claro es que el suceso contrario del imposible es el suceso seguro.

3.362. Unión

Sean los sucesos $A \subset H$ y $B \subset H$ dos sucesos de la misma categoría de pruebas. Se dice que el suceso C es su suceso-reunión, y se escribe $A \cup B = C$, si y sólo si se verifica C, cuando se verifica al menos uno de los reunidos.

Los sucesos elementales que forman el conjunto C son todos los que pertenecen a A y/o a B.

$$A = \{h_1,\ h_2,\ \ldots,\ h_j\} \qquad B = \{h_k,\ h_{k+1},\ \ldots,\ h_m\}$$
$$A \cup B = C = \{h_1,\ h_2,\ \ldots,\ h_j,\ h_k,\ h_{k+1},\ \ldots,\ h_m\}$$

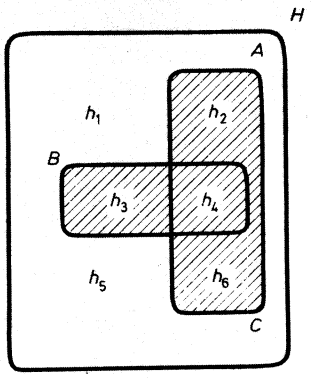
Ejemplo 8

De la categoría de pruebas del ejemplo 1, se establecen los sucesos A = «conseguir un número múltiplo de 2» y B = «obtener un número mayor que dos y menor que 5».

Usamos un diagrama de Venn que nos permite «ver» la reunión, $A \cup B$.

$$A = \{h_2,\ h_4,\ h_6\} \quad ; \quad B = \{h_3,\ h_4\}$$
$$C = A \cup B = \{h_2,\ h_3,\ h_4,\ h_6\}$$

Si sale 2, se verifica A; basta para que se verifique $A \cup B$; si aparece un 3, sucede B; basta para que se verifique $A \cup B$; si se produce un 4 se verifican A y B; sucede $A \cup B$; si resulta un 6, se verifica A; suficiente para que se realice $A \cup B$.



3.363. Intersección. Sucesos incompatibles

Sean los sucesos $A \subset H$ y $B \subset H$ dos sucesos de la misma categoría de pruebas. Se establece que el suceso C es su suceso-intersección —y se escribe $A \cap B = C$— si y solamente si se verifica C, cuando se verifican ambos sucesos intersecados.

Los sucesos elementales que forman el conjunto-intersección C son los comunes a A y a B.

$$A = \{h_1, \ldots, h_{j-1}, h_j\} \qquad B = \{h_{j-1}, h_j, h_k, \ldots, h_m\}$$
$$A \cap B = C = \{h_{j-1}, h_j\}$$

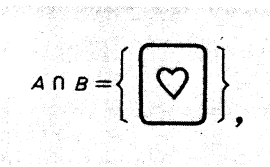
Ejemplo 9

De una baraja de 52 cartas se extrae, al azar, un naipe. Se consideran los sucesos A = «conseguir un as» y B = «obtener corazones». He aquí su constitución en sucesos elementales:

$A = \{$ ♣ , ♡ , ◇ , ♠ $\}$

$B = \{$*conseguir una de las 13 cartas de corazones*$\}$

La intersección, $A \cap B$, resulta ser unitaria en este caso:



pues el único suceso elemental, común a los sucesos intersecados, es «obtener el as de corazones».

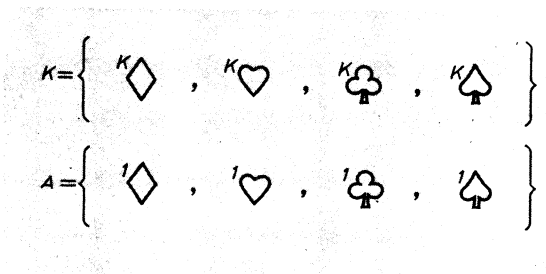
Sucesos incompatibles. Dos sucesos A y B de la misma categoría de pruebas son incompatibles si su intersección es el suceso imposible. O sea,

$$\left.\begin{array}{l} A \subset H \text{ y } B \subset H \text{ son} \\ \text{incompatibles} \end{array}\right\} \Leftrightarrow A \cap B = \phi$$

Consecuentemente, los sucesos elementales que constituyen dos sucesos incompatibles son distintos. Por ello, el que se verifique el suceso A implica que no puede suceder el B; pero adviértase que el hecho de no haberse presentado A no exige que se realice B. Puede suceder que en una prueba de su categoría no se verifique ni el uno ni el otro.

Ejemplo 10

De la categoría de pruebas del ejemplo precedente. Se consideran los sucesos K = «obtener un rey» y A = «obtener un as». He aquí dos sucesos incompatibles, constituidos por diferentes sucesos elementales



$$K \cap A = \phi$$

Si se ha verificado uno de los cuatro sucesos elementales de K, se ha verificado K, y ello prohíbe que se realice A; pero bien pudiera ser que no se obtenga un rey, lo cual no quiere decir que se haya obtenido necesariamente un as.

3.37. SISTEMA COMPLETO DE SUCESOS

Sean $H_1, H_2, \ldots, H_n$ sucesos de un espacio muestral H. Si se verifica que

1.°) $\bigcup_n H_i = H$

2.°) $H_i \cap H_j = \phi \quad , \quad \forall i \neq j,$

se dice que los n sucesos planteados forman un sistema completo de sucesos.

Tal vez se haya caído en la cuenta de que lo que se ha establecido como un sistema completo de sucesos no es más que una partición del muestral H, ya que las condiciones son las que definen la partición: un recubrimiento y la incompatibilidad (disjunción) binaria.

El más «natural» sistema completo de sucesos es el constituido por los sucesos elementales del espacio muestral

$$h_1 \cup h_2 \cup \cdots \cup h_n = H$$
$$h_i \cap h_j = \phi \quad , \quad \forall i \neq j$$

Otro sistema completo de sucesos lo constituyen siempre un suceso y su contrario, ya que

Recubrimiento: $A \cup \bar{A} = H$
Incompatibilidad: $A \cap \bar{A} = \phi$

Con estos nuevos datos, se puede establecer menos fenomenológicamente de como se hizo en 3.361, el concepto de sucesos contrarios:

> Dos sucesos son contrarios, si, siendo incompatibles, recubren el espacio muestral.

3.38. LEYES DEL ALGEBRA DE SUCESOS. EL ALGEBRA DE BOOLE DE LOS SUCESOS ESTOCASTICOS

Como se viene haciendo a lo largo del libro, a continuación se establecen las leyes más relevantes del álgebra de sucesos, respetando la enumeración y la codificación *A* o *T*, según se consideren axiomas o teoremas, siguiendo a Huntington.

De otro lado parecería reiterativo justificar todas las leyes que se establecen como teoremas (T), tanto más, cuanto que la simbología que se usa es prácticamente la conjuntista.

De un modo absolutamente general, en el capítulo 2.1, al tratar de manera abstracta el álgebra de Boole, o en los 1.1 y 1.2, referentes al álgebra proposicional y Teoría de Conjuntos, respectivamente, el lector encontrará cualquier demostración que desee verter a la nomenclatura específica de este álgebra de sucesos aleatorios; además, ello supondría, sin duda, un ejercicio más que conveniente.

T_1) *Absorción* $A \cup (A \cap B) = A \quad ; \quad A \cap (A \cup B) = A$

T_2) *Idempotencia* $A \cup A = A \quad ; \quad A \cap A = A$

T_3) *Asociatividad* $A \cup (B \cup C) = (A \cup B) \cup C \quad ; \quad A \cap (B \cap C) = (A \cap B) \cap C$

A_4) *Conmutatividad* $A \cup B = B \cup A \quad ; \quad A \cap B = B \cap A$

A_5) *Complementariedad* $A \cup \bar{A} = H \quad ; \quad A \cap \bar{A} = \phi$

A_6) *Distributividad* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad ; \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

A_7) *Identidad* $A \cup \phi = A \quad ; \quad A \cap H = A$

T_8) *Involución* $\bar{\bar{A}} = A$

Sea un suceso $B \in P(H)$.
Por complementariedad (A_5):

$$B \cup \bar{B} = H \quad ; \quad B \cap \bar{B} = \phi \qquad [1]$$

por conmutatividad (A_4):

$$\bar{B} \cup B = H \quad ; \quad \bar{B} \cap B = \emptyset \qquad [2]$$

Supóngase que $B \equiv \bar{A}$; entonces, en [2],

$$\bar{\bar{A}} \cup \bar{A} = H \quad ; \quad \bar{\bar{A}} \cap \bar{A} = \phi \qquad [3]$$

Como el axioma de complementariedad (A_5) ha de cumplirse, sucede que

$$A \cup \bar{A} = H \quad ; \quad A \cap \bar{A} = \phi \qquad [4]$$

y si el suceso contrario es único*, al comparar las expresiones [3] y [4], resulta necesariamente que

$$\bar{\bar{A}} = A$$

Consecuencia inmediata del teorema es el corolario

t_8) $$(\bar{\phi} = H) \wedge (\bar{H} = \phi)$$

T_9) *Ley de De Morgan* $\overline{(A \cup B)} = \bar{A} \cap \bar{B} \quad ; \quad \overline{(A \cap B)} = \bar{A} \cup \bar{B}$

$$[\forall h \in \overline{(A \cup B)}] \Rightarrow h \notin (A \cup B) \Rightarrow [(h \notin A) \wedge (h \notin B)] \Rightarrow$$
$$\Rightarrow [(h \in \bar{A}) \wedge (h \in \bar{B})] \Rightarrow h \in (\bar{A} \cap \bar{B}) \quad ;$$
$$\overline{(A \cup B)} \subset \bar{A} \cap \bar{B} \qquad [5]$$

recíprocamente:

$$[\forall h \in (\bar{A} \cap \bar{B})] \Rightarrow [(h \in \bar{A}) \wedge (h \in \bar{B})] \Rightarrow [(h \notin A) \wedge (h \notin B)] \Rightarrow$$
$$\Rightarrow [h \notin (A \cup B)] \Rightarrow h \in \overline{(A \cup B)} \quad ;$$
$$\bar{A} \cap \bar{B} \subset \overline{(A \cup B)} \qquad [6]$$

* En términos booleanos, la demostración de esa proposición puede hallarse en la página 117.

De [5] y de [6] se sigue la primera ley de De Morgan. Debe intentarse como ejercicio la justificación de la segunda.

T_{10}) En $[P(H), \bar{}, \cup, \cap]$ la relación de $\subset$ es de orden.

El teorema 8 de la página 119 demuestra esta proposición, en términos generales de álgebra de Boole.

Es muy conveniente que el lector se ejercite, vertiendo a las nomenclatura y formulación específicas del álgebra de sucesos, el desarrollo que allí se expone.

T_{11}) El orden $[P(H), \subset]$ tiene extremos absolutos, H y ϕ.

$\forall A \in P(H)$,

$$\begin{aligned} A \cap \phi &= \phi \cup (A \cap \phi), && \text{según } A_7 \text{ y } A_4; \\ &= (A \cap \bar{A}) \cup (A \cap \phi), && \text{según } A_5; \\ &= A \cap (\bar{A} \cup \phi), && \text{según } A_6; \\ &= A \cap \bar{A}, && \text{en virtud de } A_7; \\ &= \phi, && \text{en razón de } A_5. \end{aligned}$$

De modo que $\phi = A \cap \phi$

$$\phi = \phi \cap A, \quad \text{según } A_4$$

$$\Updownarrow$$

$$\phi \subset A$$

Por otra parte. $A = A \cap H \Leftrightarrow A \subset H$

T_{12}) *Ley de Dedekind*: $A \subset B \Rightarrow A \cup (C \cap B) \equiv (A \cup C) \cap B$

$$A \cup (C \cap B) \equiv (A \cup C) \cap (A \cup B), \quad \text{según } A_6 \qquad [7]$$

$$A \subset B \Rightarrow (A \cup B) = B \qquad [8]$$

Sustituyendo [8] en [7],

$$A \cup (C \cap B) = (A \cup C) \cap B$$

Concluyamos: El conjunto $P(H)$ de los sucesos aleatorios, con las operaciones de complementación, unión e intersección de sucesos, por cumplir las cuatro primeras leyes expuestas, es un retículo; por obedecer, además, a la quinta, es un retículo complementario; como disfruta de la distributividad dual (A_6), alcanza la estructura de retículo complementario distributivo, o lo que es igual: es un *álgebra de Boole* (consúltese el cuadro de la página 110).

3.39. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

3.390.

Ejercicios de simbolización y lectura.

Sea la experiencia que consiste en volver una ficha de las veintiocho de un dominó, que se encuentran «tapadas» sobre la mesa, y leer el número de puntos que resulta.

a) Establézcase el espacio muestral H, con sus trece sucesos elementales.
b) ¿De cuántos sucesos consta el álgebra de $P(H)$?
c) Denotando h_i el suceso que consiste en haber destapado y leído una ficha con i puntos, simbolícense o descríbanse los siguientes sucesos:

h_{13}; h_0; $\{h_0, h_1, h_2, \ldots, h_6\}$; $A = h_5 \cup h_{10}$
$B =$ «vuélvase y léase una ficha, al menos, de diez puntos»
$C =$ «consígase ficha, múltiplo de 6»
$D = \overline{h_6 \cup h_{12}}$
$E = h_4 \cap h_3$

3.391.

En la misma categoría de pruebas del ejercicio anterior, descríbanse los siguientes sucesos:

$$\bar{h}_4 \cup \bar{h}_6 \quad ; \quad \bar{h}_4 \cap \bar{h}_6 \quad ; \quad \overline{h_2 \cup \bar{h}_4}$$

3.392.

Usando las leyes del álgebra de sucesos, simplifíquese, justificando cada paso, las siguientes expresiones

a) $(A \cup B) \cap (B \cup C)$
b) $(\bar{A} \cup B) \cap (A \cup \bar{B}) \cap (A \cup B)$

3.393.

Siendo $A \in P(H)$, dibújese el diagrama de orden de los siguientes sucesos:

$$\bar{H} \cap \bar{A} \quad ; \quad \bar{H} \quad ; \quad \bar{A} \quad ; \quad \bar{H} \cup \bar{A}$$

3.394.

El departamento de verificación de una fábrica electrónica, de cada caja de 100 disyuntores, toma, al azar, tres para verificarlos en el laboratorio, y de este modo, evaluar la calidad de producción.
a) Establézcase el espacio muestral de todas las posibles tomas.
b) Tabúlese, mediante sus elementales, el suceso que consiste en haber conseguido siempre un tercer disyuntor defectuoso.

3.395.

Se lanzan dos dados homogéneos al aire. Sea el suceso $A =$ «obtener un número de puntos, múltiplo de 2» y el suceso $B =$ «obtener, al menos, un 4». ¿En qué consisten los siguientes sucesos?:

$$A \cup B \quad ; \quad A \cap B \quad ; \quad \bar{A} \cup (A \cap \bar{B})$$

3.396.

Se dispone de una urna con cuatro bolas, marcadas con los números 0, 1, 2, 3. Sea la categoría de pruebas generada por la experiencia «Extraer una bola, anotar su número, volverla a introducir y sacar una segunda bola, al azar, apuntando el número conseguido».

Establézcase el espacio muestral en sus dieciséis sucesos elementales.
Sugerencia: realícese un diagrama de árbol.

3.397.

Consúltese el capítulo 1.2, y por analogía con el álgebra de conjuntos, establézcase la diferencia de sucesos.

3.398.

De igual modo que en 3.397, defínase la diferencia simétrica de sucesos. Acompáñese el establecimiento con un diagrama de Venn.

3.399.

Demuéstrese que en el álgebra de sucesos, el contrario de todo suceso es único. Sugerencia: Consúltese el teorema 5 de la página 117.

3.4

Frecuencia y probabilidad

3.41. Introducción

3.42. Experiencias reales y simuladas. Tablas de dígitos aleatorios

3.43. Frecuencias absoluta y relativa

3.431. *Definiciones*
3.432. *Estabilización de las frecuencias. Ley del azar*
3.433. *Propiedades de las frecuencias*

3.44. Probabilidad, modelo matemático de la frecuencia

3.441. *Concepto intuitivo de probabilidad. Postulado de indiferencia. Regla de Laplace*
3.442. *Concepto axiomático de probabilidad*
3.443. *Teoremas*

3.4431. Consecuencias inmediatas de los axiomas
3.4432. Teorema de la probabilidad total

3.444. *Probabilidades condicionadas*

3.4441. Concepto
3.4442. Teorema de la probabilidad compuesta
3.4443. Independencia de sucesos
3.4444. Teorema de Bayes
3.4445. La probabilidad condicionada es una probabilidad

3.45. Técnica de resolución. Diez problemas resueltos

3.46. Aplicabilidad. Automatismos y destrezas

3.4

Frecuencia y probabilidad

3.41. INTRODUCCION

Establecido en el capítulo precedente el conjunto de los sucesos aleatorios, estructurado en álgebra de Boole, el presente capítulo se dedica a estudiar la cuantificación de su verificación dentro del espacio muestral generado por una determinada categoría de pruebas.

El método a seguir es el que siempre se utiliza en Matemáticas y que, formando un ciclo, consta de las siguientes fases:

1.ª Experimentación y observación de la realidad;
2.ª Primera abstracción, creando los objetos matemáticos;
3.ª Segunda abstracción, estructurando los objetos matemáticos;
4.ª Aplicabilidad y contraste de la teoría matemática sobre la realidad.

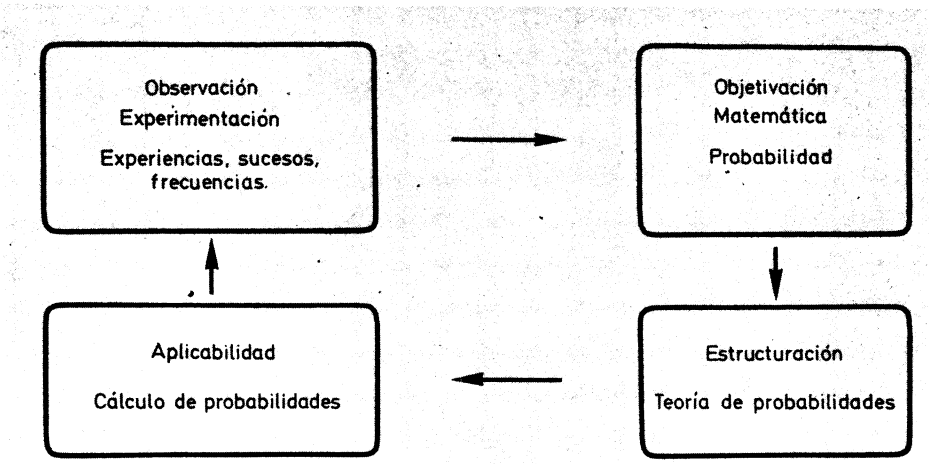
Al intentar contabilizar la verificación de un determinado suceso $h \subset P(H)$, se han de realizar pruebas y constatar resultados: es la primera fase, referible al concepto empírico de *frecuencia*.

En posesión de este empirismo, y de sus números, se intenta crear un modelo matemático que, al margen de cualquier experimentación, permita calcular «a priori», lo más aproximadamente posible, resultados aleatorios: se trata de la segunda fase, la creación del objeto matemático *Probabilidad*.

La tercera fase, segunda abstracción, consiste en estructurar axiomáticamente el conjunto de las probabilidades; postulada la base axiomática, se desarrolla la teoremática probabilística.

Finalmente, cerrando el ciclo, la aplicabilidad del modelo probabilístico sobre situaciones reales muestra la utilidad del proceso matemático para resolver la cuestión que lo suscitó: el cálculo de probabilidades sobre sucesos aleatorios. Ahí,

la *teoría de la predicción*, el concepto de *riesgo*, así como las *leyes de* los *grandes números* «acoplan» el modelo probabilístico a la realidad aleatoria de las frecuencias.



Según esto, parece inevitable iniciar el trabajo matemático con la realización (mejor, no imaginada) de las pruebas que van a dar lugar a la determinación de las frecuencias.

Tras lo dicho, ha quedado claro que esta parte de las Matemáticas es una de las que más base intuitiva tiene en sus cimientos. Las experiencias que suscitan la matematización, aquí son tan próximas, como inevitables.

Sin embargo, mientras que en otras ramas de la matemática la experiencia iniciadora del proceso de abstracción es vivencia adquirida en el normal desarrollo cultural del hombre, y no es necesario provocarlas en el momento del trabajo, en ésta del cálculo de probabilidades es muy conveniente «hacer de verdad» la experiencia, ya que, normalmente, aunque elemental no se tiene incorporada por la praxis, al acerbo cultural subconsciente.

No se quiere dejar esta breve introducción sin intentar destruir el prejuicio que considera todo lo que obedece al azar como irracional. Puede que tal error proceda del concepto vulgar de azar: todo suceso inesperado o que se realiza con sorpresa, fuera de un orden preestablecido; las Matemáticas establecen las inflexibles leyes probabilísticas a las que obedece el azar: el azar matemático.

Una parte moderna de la Matemática de la aleatoriedad es la llamada *teoría de decisiones y juegos de estrategia*. Sus conclusiones respaldan como absolutamente racionales las decisiones que se puedan tomar, basándose en las leyes del azar. Así, ha llegado hasta el gran público la extensa y rigurosa planificación realizada por determinadas marinas de guerra, que con desplazamientos «al azar» de sus submarinos nucleares, han asentado un duro golpe al espionaje desde el mar, de sus enemigos.

3.42. EXPERIENCIAS REALES Y SIMULADAS. TABLAS DE DIGITOS ALEATORIOS

Primera experiencia

Láncese una moneda al aire mil veces y constátese el resultado cara-cruz (C/F) de su reposo.

La tabla de la laboriosa experiencia se inició como se expresa y se totalizaron los resultados que se indican:

Prueba	1.ª	2.ª	3.ª	4.ª	5.ª	6.ª	7.ª	8.ª	9.ª			Total
Suceso C	1					1	1	1		...		520
Suceso F		1	1	1	1				1	...		480

Segunda experiencia

Se dispone de una urna con cinco bolas blancas (B) y cinco negras (N). Se realiza mil veces la siguiente prueba: extraer una bola, al azar, constatar su color y reintegrarla a la urna.

Los resultados fueron los que se registran:

Prueba	1.ª	2.ª	3.ª	4.ª	5.ª	6.ª	7.ª	8.ª			Total
Suceso B	1	1	1		1				...		498
Suceso N				1		1	1	1	...		502

Tercera experiencia

Se tiene un montón de cien cartulinas iguales, todas en blanco, excepto una que contiene una determinada información. Se hace mil veces la siguiente prueba: extraer una cartulina, al azar, constatar si es blanca o contiene información y reintegrarla de nuevo al montón, que se barajará concienzudamente, antes de realizar la segunda prueba.

Resultaron los sucesos que se registran y se consiguieron los totales que se tabulan.

Prueba	1.ª	2.ª	3.ª	4.ª	5.ª	6.ª	7.ª			Total
Suceso I							1	...		6
Suceso B	1	1	1	1	1		1	...		994

Método de simulación o «Monte-Carlo». Tablas de dígitos aleatorios

Ante lo engorroso y largo de la ejecución real de las experiencias y, principal-

mente, para evitar *tendencias o sesgos** en las series estadísticas de realización, se elaboran hoy las llamadas «tablas de dígitos aleatorios», de lo que se encargan los ordenadores electrónicos, convenientemente programados, para que tenga

1.° cada cifra del conjunto 0, 1, 2, . . . 9, la misma posibilidad de aparecer;
2.° los grupos de dos o más dígitos se obtengan de forma independiente.

Así, los números dados al azar por la máquina, mediante una *aplicación* que se denomina *código de simulación*, se transforman en sucesos que obedecen a leyes de probabilidad determinadas. Todo ello permite disponer de una secuencia de sucesos, de manera fácil, habiendo quedado eliminada toda posibilidad de sesgo, y en series tan largas como se quieran.

Simulación de la primera experiencia

Código de simulación: Los dígitos 0, 1, 2, 3, 4 / 5, 6, 7, 8, 9 se corresponden con C / F

Leyendo los dígitos de la primera columna de la tabla, estos son los resultados que se observan y los totalizados que se registran

Lectura	1.ª	2.ª	3.ª	4.ª	5.ª	6.ª	7.ª	8.ª	9.ª	10.ª	11.ª		Total
Suceso C							2			3			511
Suceso F	8	7	5	7	8	6		9	6		6		

Simulación de la segunda experiencia

Código de simulación: Los dígitos 0, 1, 2, 3, 4 / 5, 6, 7, 8, 9 se corresponden con B / N

Como puede comprenderse, el resultado de la simulación es idéntico al registrado en la tablilla precedente.

Simulación de la tercera experiencia

Son 100 las posibilidades de extracción de cartulinas. Si se consideran los grupos de dos dígitos, desde el 00 hasta el 99, también son 100 los que se consiguen formar. Como es una la cartulina que contiene información y 99 las que están en blanco, disponemos el siguiente código de simulación**:

* Inadvertidas sistematizaciones de realización defectuosa pueden producir sucesos «torcidos», inclinados a producirse, con preferencia, fuera del azar que se desea.

** Se está obviando toda referencia a probabilidad. Cuando llegue el momento se volverá sobre estas simulaciones y se dirá —por ejemplo— para esta experiencia 3.ª que, como la probabilidad de leer 0, 1, 2, . . . 9, es 1/10 y la computadora se ha programado para obtener de forma independiente los grupos de dígitos (segunda condición de programación), la probabilidad de cada uno de los grupos binarios 00, 01, . . . 99, es $1/10 \cdot 1/10 = 1/100$, probabilidad que coincide con la de extracción de una determinada cartulina.

El grupo de dígitos 00 / Los grupos de dígitos 01, . . . 99 — se corresponde(n) con — cartulina informativa / cartulina blanca

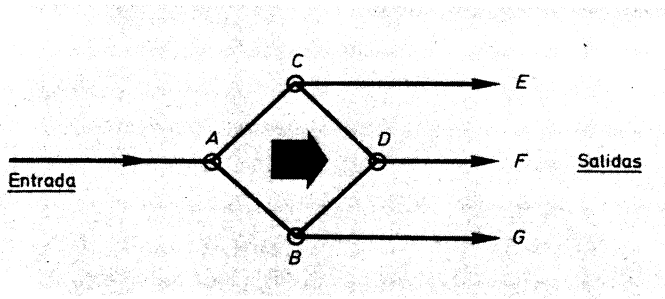
He aquí lo conseguido sobre la tabla de dígitos aleatorios (no se usa la séptima columna de cada agrupación vertical).

Lectura	1.ª 2.ª 3.ª . . . 92.ª . . . 230.ª . . . 373.ª . . .	Total
Suceso I	00 00 00	8
Suceso B	87 78 59	992

Ejemplo

*De simulación de una secuencia de experiencias, de probabilidades preestablecidas**

El núcleo viario del centro comercial de una ciudad se esquematiza en el siguiente gráfico unidireccional:



Al nudo *A* pueden acceder en cada minuto, cero, uno, dos, tres o cuatro vehículos, considerándose las dos salidas de su bifurcación con idéntica densidad de tráfico.

Del tráfico que llega a *B* y a *C*, se estima que las tres cuartas partes de cada uno de ellos se canaliza hacia *D*, escogiendo las salidas laterales *E* y *G* la cuarta parte de los vehículos que a ellos llegan.

Se desea simular la circulación viaria de esta red, durante quince minutos.

Código de simulación

Entrada: Los dígitos 0, 1 ⟶ 0 vehículos
2, 3 ⟶ 1 »
4, 5 ⟶ 2 »
6, 7 ⟶ 3 »
8, 9 ⟶ 4 »

* Remitimos a la nota anterior.

DIGITOS ALEATORIOS (I)

8758485	4798746	9966106	6607921	9952566	244107	1891548	9152326
7890021	4969192	8804964	8107053	9397643	3422379	5955485	4931498
5989617	1554221	5418770	8524631	2378858	7551463	3899056	5431170
7495513	6092549	9095674	9741103	6585554	1843391	1790361	4151646
8796622	5414917	3319900	1185141	7231747	2724210	1259537	3039334
6900167	4046991	2180440	6659721	334366	2068707	9402948	7799327
2169426	2822608	7410813	9061402	7671089	4473916	7803696	6556929
9108312	5637507	1850229	363809	5530791	9910462	9685655	8919768
6347709	7808338	9720642	8048809	807071	2403144	7155221	1303026
3421163	8799740	2007968	2850147	9029164	8523661	9879491	2563994
6468547	5735331	6195062	5552389	7558770	5381119	4257786	7116640
4379763	2228820	3955049	3670908	6430008	5541874	5381171	2410155
6030390	4490940	2672129	5614310	9636693	7291370	7017978	6485536
5751412	6138647	5069169	5167190	5380615	5778976	6248317	5479114
6639825	526924	3403119	5676399	3430321	9494334	6093111	1109654
1819927	932671	9216681	6906046	8486143	8762438	6199343	8334112
4210581	256474	3643609	9553390	4527854	1186613	6368986	7534401
7885527	9503551	6051562	777407	200386	4205648	3430411	2731634
5516107	8511930	1426618	1952337	8874454	5675693	4184068	4023165
6482379	2685768	7773307	2467764	4846817	6871020	7604769	3789428
4293647	1657032	1299364	2882895	5603090	7672479	5607064	4590075
7076868	1150535	3211394	8913545	4578720	7250410	2293977	8510172
415240	5899890	1662178	6874055	6284729	5841878	8488701	8355304
3733517	7203361	9618512	2880818	718297	8382421	3829852	7537318
4620510	1765461	9008171	8159874	7885706	3875367	2280848	8806785
2313079	4617408	6886731	9763716	6601713	1736828	1005552	401859
3361180	6550350	9051479	5355720	671004	5824542	8908213	1028401
5996486	6723309	6371475	7719068	8971128	4355155	5390772	3148239
372480	3900729	52056	5205770	766114	7744752	9573484	7738135
267450	1961479	9361825	8517636	6849391	4437623	4981216	9948690
4861194	9628952	4022964	7477214	8656606	4644709	9958795	7950388
8073168	6885513	8654568	9957786	1855601	1513533	2380788	662926
2550461	9336432	3064444	4358774	8572646	2206908	6087633	6663622
5193030	1185580	376209	1587028	6136287	2534471	9980240	7071203
2605052	1989486	8491445	3043298	1836777	3630982	5254894	8850523
5809094	5199853	8917266	6704921	9974128	9500475	7235694	7909884
2338057	2839381	5993772	408197	8505236	7357637	7598699	9373459
7852462	2753637	5849660	315221	9244388	2629334	2576510	1795052
7581719	9334847	7773610	2628033	5805704	1181922	4840193	8403861
6861426	5533808	1450012	8895798	324678	1885883	8393196	3386231
4778617	8195621	6166170	3236432	3923060	4410469	1155276	7237430
3027093	3025689	910294	8230564	1190736	3069339	7699406	8572380
2139624	5686323	4861318	7990996	4194111	3245702	1727213	1151961

Deferencia de la Escuela de Informática y Centro de Cálculo de la Universidad de Deusto.

DIGITOS ALEATORIOS (II)

1366848	7833434	4698969	7692909	3866730	3964199	8984626	8229959
8518121	7039092	5571464	76954	318545	1218684	4445199	5703038
4211439	3941286	5744766	8997019	2279221	2702153	5699928	9880185
7981760	8968890	1977498	1144976	9072372	4129447	3125328	1586945
1393719	4079808	1935373	4893962	1945411	7626802	8252114	871464
959757	7915361	8854351	1887855	1637969	2837118	2280982	8151827
8382125	6926304	6118700	4375462	1184471	7727663	5705736	4685451
6761076	8397399	9534705	1631636	3977473	9180110	9283397	3079393
4925783	1840160	6708907	3692003	1771852	7403085	8471843	4203292
8973160	6009331	5297542	7701267	8529725	1866945	4434144	9802354
8906827	5219772	1157184	9965154	9376267	6571212	5040864	1104274
1257867	7608731	4331580	7510902	6081190	8889019	8603404	1619254
2284887	9136030	4252199	3288918	1463717	9182041	1918791	8874374
5977127	5993392	2166204	9056693	4844324	7555701	1735292	2410439
8845000	1376050	8651298	9523336	9278331	9959962	6254794	7889105
1041480	5246929	2108255	5427168	3588709	2687736	3828036	8778591
8219216	307978	7874923	4477730	5992073	5652870	9988557	9055514
4436067	5116770	776018	8605176	4646893	434769	786576	806531
7759997	9301201	5967232	2092578	8850377	4269062	5960973	7344282
416931	6403043	4665877	367873	214344	7975203	5922116	3755870
9236175	1614215	6559712	4830338	9944618	6194664	7666421	246546
2481481	2669973	3686507	8089284	5357135	9339254	7821311	2874576
6855653	5262729	9875495	1888406	2450983	7710238	4202581	5823344
7116837	290922	7693995	3545666	2028041	257253	3291146	7431601
4969286	2931309	2864275	803866	9044722	7035537	798720	1490483
1754414	7112131	6883061	7289185	1787560	5122691	4648102	1784389
8873411	7180962	3225073	4721781	9305027	3334131	6259541	7550066
8964522	5836537	4338520	3502281	1967006	281508	3985991	1382376
2420333	2080609	700655	5478447	6564784	82681	1413030	7734052
3570753	8383230	8162597	3526514	7695707	4435610	7352298	4193295
8989089	6194878	6267463	1850870	4698055	1530496	6900475	7628388
3666047	3340790	7050319	2234798	9955917	9622322	8130675	2183148
9922808	9888513	25806	1158219	6717060	9878391	8816802	3995289
4620510	1765461	9008171	8159874	7885706	3875367	2280848	8806785
2313079	4617408	6886731	9763716	6601713	1736828	1005552	401859
3361180	6550350	9051479	5355720	671004	5824542	8908213	1028401
5996486	6723309	6371475	7719068	8971128	4355155	5390772	3148239
372480	3900729	52056	5205770	766114	7744752	9573484	7738135
267450	1961479	9361825	8517636	6849391	4437623	4981216	9948690
4861194	9628952	4022964	7477214	8656606	4644709	9958795	7950388
8073168	6885513	8654568	9957786	1855601	1513533	2380788	662926
2550461	9336432	3064444	4358774	8572646	2206908	6087633	6663622
5193030	1185580	376209	1587028	6136287	2534471	9980240	7071203

Bifurcación A: Los dígitos 0, 1, 2, 3, 4 → vehículos a *C*
5, 6, 7, 8, 9 → vehículos a *B*

Birfurcaciones C y B: Los grupos de dígitos

00, . . . 24 → vehículos a salidas laterales *E* o *G*
25, . . . 99 → vehículos hacia el nudo *D*

Registro de simulación

Minuto	*Entradas*		*Bifurcación A*		*Bifurcaciones C, B*	
	Dígito	*Vehículos*	*Dígitos*	*Dirección*	*Dígitos*	*Dirección*
1	8	4	8-7-5-7	*B-B-B-B*	87-78-59-74	*D-D-D-D*
2	7	3	8-6-2	*B-B-C*	87-69-21	*D-D-E*
3	5	2	9-6	*B-B*	91-63	*D-D*
4	7	3	3-6-4	*C-B-C*	34-64-43	*D-D-D*
5	8	4	6-5-6-1	*B-B-B-C*	60-57-66-18	*D-D-D-E*
6	6	3	4-7-5	*C-B-B*	42-78-55	*D-D-D*
7	2	1	6	*B*	64	*D*
8	9	4	4-7-0-3	*C-B-C-C*	42-70-04-37	*D-D-E-D*
9	6	3	4-2-3	*C-C-C*	46-23-33	*D-E-D*
10	3	1	5	*B*	59	*D*
11	6	3	0-0-4	*C-C-C*	03-02-48	*E-E-D*
12	4	2	8-2	*B-C*	80-25	*D-D*
13	6	3	5-2-5	*B-C-B*	51-26-58	*D-D-D*
14	5	2	2-7	*C-B*	23-78	*E-D*
15	6	3	7-6-4	*B-B-C*	75-68-47	*D-D-D*

Algunas conclusiones

Han circulado en esos quince minutos cuarenta y un vehículos.
El máximo de entradas lo registran los minutos primero, quinto y octavo; y el mínimo, los minutos séptimo y décimo.
En cada minuto han entrado, al menos, un vehículo.
La calle *AC* la han utilizado dieciocho vehículos; y la *AB*, veintitrés.
Han confluido en *D* treinta y cuatro coches, que han salido por *F*
La salida *G* no se ha utilizado y la *E* la usaron siete vehículos.

3.43. FRECUENCIAS ABSOLUTA Y RELATIVA

3.431. Definiciones

Sea el suceso *A* un subconjunto del espacio muestral *H*; entonces, $A \in P(H)$. Si en una serie de *n* pruebas se ha presentado el suceso *A* n' veces, diremos que

la frecuencia absoluta de A es n', y su frecuencia relativa n'/n. Los dos conceptos se denotan así:

$$n(A) = n' \quad ; \quad h(A) = \frac{n'}{n}$$

Es claro que, con toda generalidad, sucede que $n_i = h_i \cdot n$.

También resulta evidente que la suma de las frecuencias absolutas de todos los sucesos presentados en una serie de n pruebas ha de ser igual a n,

$$\Sigma n_i = n$$

La frecuencia relativa de un suceso, h_i, puede expresarse —según convenga— en tanto por uno, tanto por ciento, tanto por mil o partes por millón.

Ejemplo

La frecuencia relativa de un suceso que en cincuenta pruebas se ha presentado diez veces es

$$h = \frac{10}{50} = 0{,}2 \sim 20\,\% \sim 200\,‰ \sim 200\,000 \text{ ppm}$$

Ejercicio

Establézcanse las frecuencias relativas $h(C)$, $h(N)$ y $h(I)$, referibles a los sucesos de las experiencias del número 3.42.

3.432. Estabilización de las frecuencias. Ley del azar

Sea el suceso C = «obtener cara» en la categoría de pruebas «lanzar una moneda al aire y observar su cara superior en reposo».

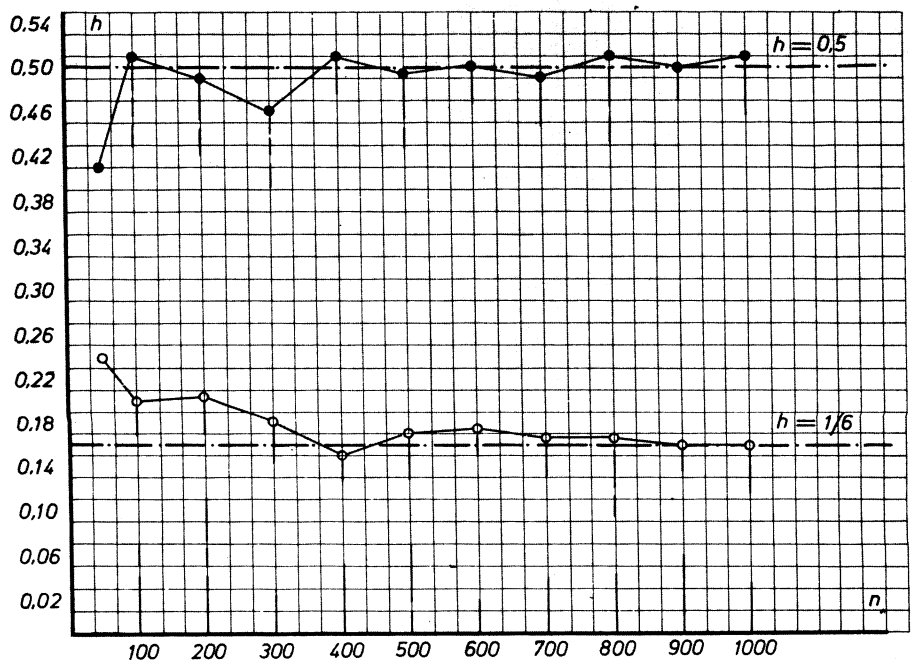
Se tabulan las frecuencias absolutas $n(C)$ y relativas $h(C)$, en función del número de pruebas realizadas, n.

Número de pruebas n	*Frecuencia absoluta* $n(C)$	*Frecuencia relativa* $h(C) = n(C)/n$
100	51	0,51
200	98	0,49
300	140	0,46
400	205	0,51
500	249	0,495
600	302	0,50
700	340	0,485
800	410	0,51
900	455	0,50
1 000	511	0,511

Se realiza ahora la prueba «lanzar un dado homogéneo sobre la mesa y leer su cara superior en reposo». Se han conseguido los siguientes números, referidos al suceso E = «Obtener y leer dos puntos».

n	$n(E)$	$h(E)$
100	20	0,2
200	41	0,205
300	50	0,166
400	62	0,155
500	85	0,170
600	104	0,173
700	117	0,167
800	134	0,167
900	151	0,165
1 000	165	0,165

Sobre la columna de las frecuencias relativas de los dos ejemplos desarrollados y, mejor aún, sobre las gráficas que se dibujan a continuación, puede observarse que, a medida que se eleva el número de pruebas, n, las frecuencias, h, «tienden» a estabilizarse alrededor de un valor determinado, que en el caso de las monedas es 0,5 y en el de los dados, 1/6.



Esta «tendencia» constituye la *Ley del azar*, que dicta:

> En series largas de pruebas, la frecuencia relativa de un suceso «tiende» a estabilizarse alrededor de un número, que coincide con su probabilidad.

Tal formulación resulta de lo más indeseable en Matemáticas y ello, entre otras, por estas dos razones:

a) no explicita cuánto se aproxima la frecuencia a la probabilidad, ni cuál ha de ser la longitud de la serie para conseguir una determinada aproximación;
d) de ningún modo, una justificación empírica demuestra una proposición.

Sin embargo, puede admitirse sin recelos esta Ley del azar, pues J. Bernoulli, en 1713, al demostrar la «Ley débil de los grandes números», solventó las dificultades apuntadas, respaldando de este modo el empirismo de la ley del azar.

3.433. Propiedades de las frecuencias

I. La frecuencia relativa de un suceso A, es un racional del cerrado $[0, 1]$
En efecto: siendo n el número de pruebas realizadas y $n(A)$ la frecuencia absoluta de A, es claro que

$$0 \leq n(A) \leq n;$$

dividiendo por n

$$0 \leq \frac{n(A)}{n} \leq 1;$$

o sea:

$$\boxed{0 \leq h(A) \leq 1}$$

II. Las frecuencias relativas del suceso seguro y del suceso imposible son, respectivamente, 1 y 0.
Si H es el suceso seguro, realizadas n pruebas, se ha presentado n veces; luego, $n(H) = n$, y

$$\boxed{h(H) = n/n = 1} \quad ;$$

por definición, el suceso imposible no se ha presentado ninguna vez en las pruebas, luego

$$\boxed{h(\phi) = 0/n = 0}$$

III. La frecuencia relativa del suceso-reunión de dos incompatibles es igual a la suma de las frecuencias relativas de los sucesos reunidos.
Sean los sucesos A y B incompatibles: $A \cap B = \phi$.
Sus frecuencias absolutas en n pruebas son:

$$n(A) = n_1$$
$$n(B) = n_2$$

Para que se presente el suceso-reunión, $A \cup B$, habrá de presentarse A o B, y nunca ambos, por ser incompatibles; de modo que

$$n(A \cup B) = n_1 + n_2$$
$$h(A \cup B) = \frac{n_1 + n_2}{n} = n_1/n + n_2/n;$$

$$\boxed{h(A \cup B) = h(A) + h(B)}$$

3.44. PROBABILIDAD, MODELO MATEMATICO DE LA FRECUENCIA

3.441. Concepto intuitivo de probabilidad. Postulado de indiferencia. Regla de Laplace

Antes de nada, quede claro que el concepto que se desarrolla en este número es completamente insuficiente, desde un punto de vista matemático, porque, como se verá en seguida, no se respetan las más elementales reglas de definición, como es que «en la definición no puede entrar el término definido». Habrá que esperar al siguiente número, en el que se desarrolla el concepto de probabilidad axiomáticamente, desde un punto de vista rigurosamente matemático.

Sensibilizado el concepto de probabilidad como la frecuencia de un suceso, cuando el número de pruebas se repite «ilimitadamente», considérese un espacio muestral H formado por n sucesos *equiprobables o incompatibles*; es decir, un sistema completo de sucesos:

$$H = \{h_1, h_2, \ldots h_n\}$$

Según lo establecido, sus probabilidades cumplen las siguientes expresiones:

$$p(H) = 1$$

$$\left.\begin{array}{l} p(h_1) + p(h_2) + \ldots + p(h_n) = 1 \\ p(h_1) = p(h_2) = \ldots = p(h_n) \end{array}\right\} \Rightarrow p(h_i) = \frac{1}{n}$$

Si un suceso $A \in P(H)$, se obtiene mediante la reunión de los m incompatibles

$$A = h_1 \cup h_2 \cup \ldots \cup h_m,$$

sucede que

$$p(A) = p(h_1) + p(h_2) + \ldots + p(h_m)$$
$$p(A) = \frac{1}{n} + \frac{1}{n} + \ldots (m \text{ veces}$$

$$\boxed{p(A) = \frac{m}{n}}$$

La expresión recuadrada constituye la regla de Laplace, que dice:

> La probabilidad de un suceso es el cociente entre los casos favorables (éxitos) y casos posibles, considerados *equiprobables e incompatibles*.

Ejemplo 1

¿Qué probabilidad existe de obtener un número múltiplo de 3, al lanzar un dado homogéneo sobre la mesa?

$$H = \{h_1, h_2, h_3, h_4, h_5, h_6\}$$
$$p(h_1) = p(h_2) = \ldots = p(h_6) = \frac{1}{6}$$
$$A = h_3 \cup h_6$$
$$p(A) = \frac{1}{6} + \frac{1}{6} = \frac{1}{3};$$

o lo que es igual: casos favorables = 2
casos posibles = 6

$$p(A) = \frac{2}{6} = \frac{1}{3}$$

Ejemplo 2

¿Qué probabilidad hay de conseguir 4 puntos, al levantar una ficha de dominó?

casos posibles: 28
casos favorables: 0 + 4
1 + 3
2 + 2

$$p(A) = \frac{3}{28}$$

3.442. Concepto axiomático de probabilidad

Inaceptable el concepto intuitivo de probabilidad, por las razones expuestas anteriormente, Kolmogorov, en 1933, estableció definitivamente la probabilidad de un modo axiomático.

Sea H el espacio muestral y $P(H)$ —el conjunto de sus partes—, el universal al que pertenecen todos los sucesos del discurso.

Se denomina probabilidad a una aplicación de $p(H)$ en el conjunto de los números reales, $\mathfrak{R}$,

$$P(H) \xrightarrow{P} \mathfrak{R},$$

que obedece a los siguientes axiomas:

I. $\forall A \in P(H), \quad 0 \leq p(A) \leq 1$*
II. $p(H) = 1$
III. $A \in P(H), \ B \in P(H) \,/\, A \cap B = \phi \Rightarrow p(A \cup B) = p(A) + p(B)$

Si en lugar de definir la aplicación sobre $\mathfrak{R}$, se define sobre el cerrado real $[0, 1]$ el axioma 1 debe suprimirse.

3.443. Teoremas

3.4431. *Consecuencias inmediatas de los axiomas*

1) La probabilidad del suceso contrario de otro es igual a la unidad menos la probabilidad del directo.

Los sucesos contrarios A y $\bar{A}$ forman un sistema completo de sucesos; por tanto,

$$A \cup \bar{A} = H$$
$$p(H) = p(A) + p(\bar{A})$$
$$1 = p(A) + p(\bar{A})$$

$$\boxed{p(\bar{A}) = 1 - p(A)}$$

Como corolario de este teorema, resulta que

$$\boxed{p(\phi) = 0}$$

En efecto:

$$\bar{H} \equiv \phi$$

$$p(\bar{H}) = 1 - p(H) = 1 - 1 = 0$$

---

* En rigor, debería escribirse solamente $0 \leq p(A)$, puesto que la cota superior se puede deducir *teoremáticamente*.

2) Si el suceso A está incluido en el B, entonces la probabilidad de A es menor o igual que la de B

$$A \subset B \Rightarrow p(A) \leq p(B)$$

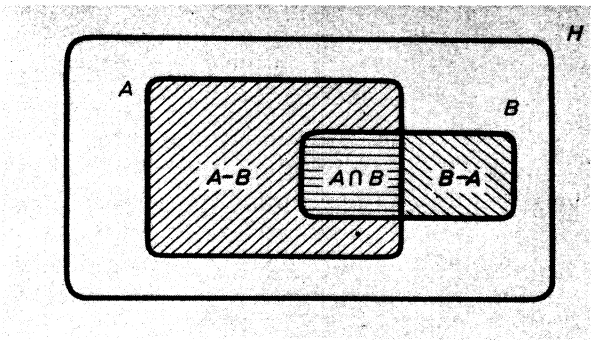
Su elemental justificación se deja como ejercicio para el lector.

3.4432. *Teorema de la probabilidad total*

La probabilidad del suceso-reunión de dos sucesos es igual a la suma de las probabilidades de los reunidos, menos la de su intersección. Simbólicamente:

$$\forall A \in p(H),\ \forall B \in P(H),\ p(A \cup B) = p(A) + p(B) - p(A \cap B)$$

Para su demostración ha de usarse el teorema-extensión del axioma III, pero, para poderlo aplicar, ha de establecerse el suceso $A \cup B$ como reunión de sucesos incompatibles y, entonces, se podrá establecer que la probabilidad de la reunión es la suma de las probabilidades de los reunidos.



El álgebra de sucesos justifica de manera elemental lo que expresa el diagrama de Venn de la figura; o sea, que

$$(A \cup B) = (A - B) \cup (B - A) \cup (A \cap B).$$

Al ser incompatibles los tres sucesos reunidos, el teorema-extensión del axioma III permite establecer

$$p(A \cup B) = p(A - B) + p(B - A) + p(A \cap B) \qquad [1]$$

Del mismo modo, los sucesos A y B están constituidos por la reunión de incompatibles,

$$A = (A - B) \cup (A \cap B) \quad ; \quad B = (B - A) \cup (A \cap B),$$

lo que permite escribir para sus probabilidades (axioma III),

$$\begin{aligned} p(A) &= p(A - B) + p(A \cap B) \\ p(B) &= p(B - A) + p(A \cap B) \end{aligned}$$

$$p(A) + p(B) = p(A - B) + p(B - A) + p(A \cap B) + p(A \cap B) \qquad [2]$$

Sustituyendo [1] en [2],

$$p(A) + p(B) = p(A \cup B) + p(A \cap B);$$

despejando,

$$\boxed{p(A \cup B) = p(A) + p(B) - p(A \cap B)}$$

Claro es que el resultado del teorema se muestra acorde con el axioma III, si se trata de sucesos incompatibles, ya que, entonces, el tercer término del segundo miembro de la fórmula se anula, $p(\phi) = 0$.

Así, pues, la expresión recuadrada es del todo general y sirve tanto para sucesos compatibles como incompatibles.

La asociatividad del álgebra de sucesos permite generalizar la fórmula para más de dos sucesos. Se brinda al lector, como ejercicio, la demostración del teorema para tres sucesos, cuya conclusión ha de ser

$$p(A \cup B \cup C) = p(A) + p(B) + p(C) - p(A \cap B) - p(A \cap C) - p(B \cap C) + p(A \cap B \cap C)$$

Ejemplo 1.

¿Qué probabilidad hay de que al levantar una ficha de dominó se obtenga un número de puntos mayor que 9 o un múltiplo de 4?

Los veintiocho sucesos elementales posibles se tabulan en el siguiente cuadro:

	0	1	2	3	4	5	6
0	00	10	20	30	40	50	60
1	xx	11	21	31	41	51	61
2	xx	xx	22	32	42	52	62
3	xx	xx	xx	33	43	53	63
4	xx	xx	xx	xx	44	54	64
5	xx	xx	xx	xx	xx	55	65
6	xx	xx	xx	xx	xx	xx	66

$$A = \{n > 9\} = \{(4 \cdot 6),\ (5 \cdot 5),\ (5 \cdot 6),\ (6 \cdot 6)\}$$
$$B = \{n = 4\} = \{(0 \cdot 4),\ (1 \cdot 3),\ (2 \cdot 2),\ (2 \cdot 6),\ (3 \cdot 5),\ (4 \cdot 4),\ (6 \cdot 6)\}$$
$$A \cap B = \{(6 \cdot 6)\}$$

$$p(A \cup B) = \frac{4}{28} + \frac{7}{28} - \frac{1}{28} = \frac{10}{28} = \frac{5}{14}$$

El resultado es coincidente con el obtenido si se plantea directamente el suceso-reunión, $A \cup B$, formado por once sucesos elementales:

$$\left.\begin{array}{l}\text{casos favorables: } 10\\ \text{casos posibles: } 28\end{array}\right\} \Rightarrow p(A \cup B) = \frac{10}{28} = \frac{5}{14}$$

Ejemplo 2

A un simposio de Ecología asisten cien congresistas, de los cuales, ochenta hablan inglés y cuarenta francés. ¿Qué probabilidad existe de que dos especialistas, escogidos al azar, se entiendan sin intérprete?

Sea el suceso I = «entenderse en inglés» y el F = «entenderse en francés». Es claro que el suceso del problema es «ENTENDERSE», lo que pueden hacer en inglés o en francés; es decir, la probabilidad pedida es la del suceso $(I \cup F)$.

De los datos del problema se infiere que hay congresistas bilingües, que dan lugar al suceso «entenderse en inglés y en francés», a saber, al suceso $(I \cap F)$.

El número de bilingües es:

$$\text{card}(I \cup F) = \text{card}(I) + \text{card}(F) - \text{card}(I \cap F);$$
$$100 = 80 + 40 - \text{card}(I \cap F) \quad ; \quad \text{card}(I \cap F) = 20$$

Probabilidad de entenderse en inglés

Casos favorables: todas las parejas que se puedan formar con los ochenta especialistas que dominan ese idioma

$$\binom{80}{2}$$

Casos posibles: todas las parejas distintas que se pueden formar con los cien congresistas: $\binom{100}{2}$

$$p(I) = \frac{\binom{80}{2}}{\binom{100}{2}}$$

Probabilidad de entenderse en francés

Casos favorables: $\binom{40}{2}$

Casos posibles: $\binom{100}{2}$

$$p(F) = \frac{\binom{40}{2}}{\binom{100}{2}}$$

Probabilidad de entenderse en francés y en inglés

Casos favorables: $\binom{20}{2}$

Casos posibles: $\binom{100}{2}$

$$p(I \cap F) = \frac{\binom{20}{2}}{\binom{100}{2}}$$

Probabilidad de «ENTENDERSE» sin intérprete (T. de la probabilidad total)

$$p(I \cup F) = \frac{\binom{80}{2}}{\binom{100}{2}} + \frac{\binom{40}{2}}{\binom{100}{2}} - \frac{\binom{20}{2}}{\binom{100}{2}} = \frac{3\,160 + 780 - 190}{4\,950} = 0{,}757$$

3.444. Probabilidades condicionadas

3.4441. *Concepto*

Sean A y B dos sucesos compatibles, no imposibles, procedentes de la misma categoría de pruebas.

$$A \in P(H), \quad B \in P(H), \quad A \neq \phi, \quad B \neq \phi; \quad A \cap B \neq \phi$$

Entiéndase que A es el subconjunto de H, formado por los i sucesos elementales

$$A = \{h_1, h_2, \ldots h_i\}$$

Se denomina probabilidad de B condicionada a A —denotada $p(B/A)$— a la probabilidad de B sobre el espacio probabilístico* A.

La anterior definición significa que se ha verificado A, puesto que es el nuevo universal estocástico. Tal vez ayude a comprender el establecimiento el siguiente

Ejemplo

Una jaula de lotería contiene 10 bolas de corcho, numeradas con las cifras 0, 1, . . . 9, y otras cinco, de hierro, con las cinco primeras marcas numéricas de las anteriores. Todas las bolas son de idéntica apariencia y no se tiene acceso a ellas.

Tras las vueltas reglamentarias, se vierte una bola sobre un pocillo especial, transparente, lleno de agua; y sólo se puede observar que se hunde. Consecuentemente, se sabe que la bola vertida es de hierro.

El problema consiste en esto: ¿Qué probabilidad hay de que la bola sumergida sea un 4?

Analicemos despacio la respuesta:

a) Nominemos los sucesos así:

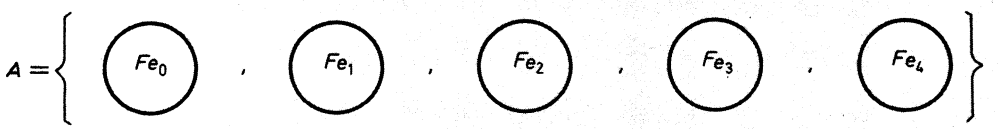
A = «obtener bola de hierro»
B = «conseguir bola marcada con un 4»

Ambos sucesos pertenecen al espacio probabilístico, H, formado por los quince sucesos posibles. Sus probabilidades sobre H son

$$p(A) = 5/15 = 1/3; \quad p(B) = 2/15;$$

* Recibe este nombre todo espacio muestral booleano sobre el que se ha definido la aplicación «*probablidad*».

b) Pero el hecho observado (la sumergibilidad de la bola) hace que el suceso cuya probabilidad se pide ya no pertenezca a la categoría de pruebas anteriormente apuntada; su espacio probabilístico ya no es H, con sus 15 sucesos elementales, sino que —por haberse producido A— ése es, precisamente, el muestral del problema



$$\left.\begin{array}{l}\text{casos favorables: } 1\\ \text{casos posibles: } 5\end{array}\right\} p(B/A) = \frac{1}{5}$$

La probabilidad de que, habiendo conseguido bola de hierro, esté marcada con un 4 es 1/5.

3.4442. *Teorema de la probabilidad compuesta*

La probabilidad del suceso-intersección de dos no imposibles es igual al producto de la probabilidad de uno de ellos por la del otro, condicionada a él.

Sea el espacio probabilístico $H = \{h_1, h_2, \ldots h_n\}$, constituido por n sucesos elementales.

Considérese el suceso $A \subset H$, formado por n_1 sucesos elementales, de los n de H; y el suceso $B \subset H$, con n_2 sucesos elementales, de los n del muestral.

Finalmente, sea $A \cap B \subset H$ un suceso constituido por n_3 sucesos elementales de los de H.

Es claro entonces que las probabilidades respectivas son:

$$p(A) = n_1/n \quad ; \quad p(B) = n_2/n \quad ; \quad p(A \cap B) = n_3/n$$

De otro lado, considérese el suceso B/A, que, como se dijo, ya no pertenece a la misma categoría de pruebas que los anteriores, puesto que su espacio muestral es A.

Casos favorables de B/A: son aquellos en los que, habiéndose presentado A, también lo hace B; obviamente son n_3.

Casos posibles de B/A: los de su espacio muestral: n_1

$$p(B/A) = n_3/n_1$$

dividiendo numerador y denominador por n,

$$p(B/A) = \frac{n_3/n}{n_1/n} = \frac{p(A \cap B)}{p(A)} \qquad [1]$$

> La probabilidad de un suceso condicionado a otro es igual al cociente de la probabilidad de su intersección y la del condicionante.

Puede despejarse de la expresión [1] la probabilidad de la intersección, resultando

$$\boxed{p(A \cap B) = p(A) \cdot p(B/A)} \qquad [1\,']$$

cuya lectura corresponde al enunciado con que se inició este epígrafe.

Ejemplo

¿Qué probabilidad hay de que, habiendo extraído de una baraja de 52 naipes una carta «corazones», sea figura?

A = «corazones» ; B = «figura» ; $A \cap B$ = «figura de corazones»

$$p(A) = 13/52 = 1/4 \quad ; \quad p(A \cap B) = 3/52$$

$$p(B/A) = \frac{3/52}{13/52} = 3/13$$

3.4443. *Independencia de sucesos*

Dos sucesos A y B de un mismo espacio probabilístico son *independientes* si

$$p(B) = p(B/A),$$

siendo *dependientes* en caso contrario.

Ejemplo 1

En la categoría de pruebas «lanzar un dado al aire y leer su cara superior en reposo» se consideran los sucesos A = «obtener un número mayor que 4» y B = = «conseguir un múltiplo de 3»; o sea:

$$H = \{h_1, h_2, h_3, h_4, h_5, h_6\}$$
$$A = \{h_5, h_6\} \quad ; \quad B = \{h_3, h_6\}$$
$$B \cap A = \{h_6\}$$
$$\left.\begin{array}{l} p(A) = 2/6 = 1/3 \quad ; \quad p(B) = 2/6 = 1/3 \\ p(B/A) = \dfrac{p(B \cap A)}{p(A)} = \dfrac{1/6}{1/3} = 1/2 \end{array}\right\} p(B) \neq p(B/A)$$

A y B son sucesos dependientes.

Ejemplo 2

En la misma categoría de pruebas del ejercicio anterior, sean los sucesos A = «obtener un número impar» y B = «conseguir un número mayor o igual a 5»

$$A = \{h_1, h_3, h_5\} \quad ; \quad B = \{h_5, h_6\}$$
$$B \cap A = \{h_5\}$$
$$\left.\begin{array}{l} p(A) = 3/6 = 1/2 \quad ; \quad p(B) = 2/6 = 1/3 \\ p(B/A) = \dfrac{p(B \cap A)}{p(A)} = \dfrac{1/6}{1/2} = 1/3 \end{array}\right\} p(B) = p(B/A)$$

A y B son sucesos independientes.

TEOREMA 1. La relación de independencia de sucesos en el espacio probabilístico (H, p) es simétrica; es decir:

$$\forall A \subset H, \quad \forall B \subset H, \quad p(B) = p(B/A) \Leftrightarrow p(A) = p(A/B)$$

En efecto:

$A) \Rightarrow$

$$p(A/B) = \frac{p(A \cap B)}{p(B)} \qquad [1]$$
$$p(A \cap B) = p(A) \cdot p(B/A) \qquad [2]$$

sustituyendo [2] en [1],

$$p(A/B) = \frac{p(A) \cdot p(B/A)}{p(B)},$$

y por hipótesis,

$$p(A/B) = p(A).$$

$B) \Leftarrow$

$$p(B/A) = \frac{p(B \cap A)}{p(A)} \qquad [3]$$
$$p(B \cap A) = p(B) \cdot p(A/B) \qquad [4]$$

sustituyendo [4] en [3],

$$p(B/A) = \frac{p(B) \cdot p(A/B)}{p(A)},$$

y por hipótesis,

$$p(B/A) = p(B).$$

TEOREMA 2. Dos sucesos incompatibles, no imposibles, nunca son independientes; o sea:

$$A \subset H, \quad B \subset H, \quad A \cap B = \phi \Rightarrow p(B/A) \neq p(B)$$

En efecto:

$$A \cap B = \phi \Rightarrow p(A \cap B) = 0;$$

entonces,

$$p(B/A) = \frac{p(B \cap A)}{p(A)} = 0.$$

Como $p(B) \neq 0$, es claro que

$$p(B/A) \neq p(B), \text{ c. q. d.}$$

TEOREMA 3. Inversión de condiciones.

El teorema de la probabilidad compuesta permite escribir para dos sucesos A y B, de la misma categoría de pruebas:

$$\begin{array}{ccc} p(B/A) = \dfrac{p(A \cap B)}{p(A)} & ; & p(A/B) = \dfrac{p(A \cap B)}{p(B)} \\ \Downarrow & & \Downarrow \\ p(A \cap B) = p(A) \cdot p(B/A) & ; & p(A \cap B) = p(B) \cdot p(A/B) \end{array}$$

Igualando,

$$p(B/A) = \frac{p(B)}{p(A)} \cdot p(A/B);$$

puesta de la forma

$$\boxed{\frac{p(B/A)}{p(B)} = \frac{p(A/B)}{p(A)}}$$

aparece una fórmula muy utilizada en la teoría de la información.

3.4444. *Teorema de Bayes*

El teorema de Bayes resuelve el llamado «problema de la probabilidad de las causas», que consiste en lo siguiente*:

Establecidos:

a) Un espacio probabilístico $H = \{h_1, h_2, h_3\}$

$$h_1 \cup h_2 \cup h_3 = H$$
$$h_1 \cap h_2 = h_1 \cap h_3 = h_2 \cap h_3 = \phi$$

* Se considera oportuno realizar todo el desarrollo con un espacio probabilístico de tres sucesos. La generalización a n sucesos constitutivos, sin aportar nada nuevo, obligaría a una farragosa notación, que tal vez dificultara la comprensión.

b) **Probabilidades «a priori»**

$$p(h_1) \; ; \; p(h_2) \; ; \; p(h_3)$$

c) **Un suceso** $A \subset H$

d) **Probabilidades condicionadas o *verosimilitudes***

$$p(A/h_1) \; ; \; p(A/h_2) \; ; \; p(A/h_3)$$

Pretensiones: Conocer las probabilidades «a posteriori»

$$p(h_1/A) \; ; \; p(h_2/A) \; ; \; p(h_3/A)$$

Cálculo de la probabilidad «a posteriori» $p(h_1/A)$

1.° Según el teorema de la probabilidad compuesta

$$p(h_1 \cap A) = p(h_1) \cdot p(A/h_1)$$
$$p(A \cap h_1) = p(A) \cdot p(h_1/A)$$

2.° Por ser conmutativa la intersección de sucesos,

$$p(A) \cdot p(h_1/A) = p(h_1) \cdot p(A/h_1);$$

despejando,

$$p(h_1/A) = \frac{p(h_1) \cdot p(A/h_1)}{p(A)} \qquad [1]$$

3.° $A = A \cap H = A \cap (h_1 \cup h_2 \cup h_3) = (A \cap h_1) \cup (A \cap h_2) \cup (A \cap h_3)$

4.° Las tres intersecciones son sucesos incompatibles; por tanto,

$$p(A) = p(A \cap h_1) + p(A \cap h_2) + p(A \cap h_3)$$

5.° Según el teorema de la probabilidad compuesta y conmutatividad de la intersección de sucesos,

$$\left.\begin{array}{l} p(A \cap h_1) = p(h_1 \cap A) = p(h_1) \cdot p(A/h_1) \\ p(A \cap h_2) = p(h_2 \cap A) = p(h_2) \cdot p(A/h_2) \\ p(A \cap h_3) = p(h_3 \cap A) = p(h_3) \cdot p(A/h_3) \end{array}\right\} +$$

$$p(A) = p(h_1) \cdot p(A/h_1) + p(h_2) \cdot p(A/h_2) + p(h_3) \cdot p(A/h_3) \qquad [2]$$

Sustituyendo [2] en [1],

$$p(h_1/A) = \frac{p(h_1) \cdot p(A/h_1)}{p(h_1) \cdot p(A/h_1) + p(h_2) \cdot p(A/h_2) + p(h_3) \cdot p(A/h_3)}$$

De igual modo se calcularían $p(h_2/A)$ y $p(h_3/A)$.

Entendiendo que el sistema completo de sucesos planteado, fuera de n sucesos, la fórmula de Bayes, en su forma general, es

$$p(h_i/A) = \frac{p(h_i) \cdot p(A/h_i)}{\sum_{j=1}^{j=n} p(h_j) \cdot p(A/h_j)}$$

Ejemplo

Se tiene una batería de cinco bolsas opacas, idénticas, contenedoras de bolas iguales, según estos datos:

bolsa A = cuatro bolas blancas
bolsa B = tres bolas blancas y una negra
bolsa C = dos bolas blancas y dos negras
bolsa D = una blanca y tres negras
bolsa E = cuatro bolas negras.

Con los ojos vendados, se toma una bola de una de las bolsas, advirtiéndose, luego de la extracción, que se trata de una bola negra.

¿Cuáles son las probabilidades de que proceda de cada una de las cinco bolsas?

Las probabilidades de obtener bola de una de las cinco bolsas son:

$$p(A) = p(B) = p(C) = p(D) = p(E) = 1/5$$

Las verosimilitudes respectivas son:

$$p(N/A) = 0/4 \ ; \ p(N/B) = 1/4 \ ; \ p(N/C) = 2/4 \ ; \ p(N/D) = 3/4 \ ; \ p(N/E) = 1$$

Según Bayes, las probabilidades *a posteriori*, es decir, las probabilidades de que, siendo bola negra, proceda de cada una de las bolsas son:

$$p(A/N) = \frac{1/5 \cdot 0}{1/5(0 + 1/4 + 2/4 + 3/4 + 1)} = 0 \ ; \ p(B/N) = 1/10$$

$$p(C/N) = 2/10 \ ; \ p(D/N) = \frac{1/5 \cdot 3/4}{1/5(0 + 1/4 + 2/4 + 3/4 + 1)} = 3/10$$

$$p(E/N) = 4/10$$

3.4445. *La probabilidad condicionada es una probabilidad*

No debe sorprender el título del epígrafe. Se ha establecido lo que hemos llamado «probabilidad condicionada» y, si se es consecuente, se habrá de justificar, si con ello continuamos dentro del concepto de espacio probabilístico o si, por el contrario, el nuevo objeto matemático no obedece a la axiomática definitoria de la probabilidad.

Ciertamente, las probabilidades condicionadas son probabilidades. En efecto:

I. $p(B/A) \in [0, 1]$,

ya que la probabilidad condicionada es el cociente entre dos reales positivos, siendo el numerador menor o igual que el denominador:

$$A \cap B \subset B \Rightarrow p(A \cap B) \leq p(B)$$

II. $p(H/A) = 1$

Efectivamente:

$$p(H/A) = \frac{p(H \cap A)}{p(A)} = \frac{p(A)}{p(A)} = 1$$

III. Si $B_1 \cap B_2 = \phi$, entonces $p(B_1 \cup B_2/A) = P(B_1/A) + p(B_2/A)$,

puesto que

$$p(B_1 \cup B_2/A) = \frac{p[(B_1 \cup B_2) \cap A]}{p(A)} = \frac{p[(B_1 \cap A) \cup (B_2 \cap A)]}{p(A)};$$

sucediendo que $B_1 \cap B_2 = \phi \Rightarrow (B_1 \cap A) \cap (B_2 \cap A) = \phi$, se puede escribir:

$$p(B_1 \cup B_2/A) = \frac{p(B_1 \cap A) + p(B_2 \cap A)}{p(A)} = p(B_1/A) + p(B_2/A)$$

3.45. TECNICA DE RESOLUCION. DIEZ PROBLEMAS RESUELTOS

3.450. *Una urna contiene tres bolas blancas y dos negras. ¿Cuál es la probabilidad de que dos bolas, extraídas al azar, sean ambas blancas?*

a) *Simultáneamente*

$$p = \frac{\binom{3}{2}}{\binom{5}{2}} = \frac{3}{10}$$

b) *Sucesivamente*:

H_1: extraer bola blanca la primera vez
H_2: extraer bola blanca la segunda vez
$H_1 \cap H_2$: extraer bola blanca y bola blanca

$$p(H_1 \cap H_2) = p(H_1) \cdot p(H_2/H_1)$$

H_1 y H_2 son sucesos independientes: $p(H_2/H_1) = p(H_2)$

$$p(H_1 \cap H_2) = p(H_1) \cdot p(H_2) = \frac{3}{5} \cdot \frac{2}{4} = \frac{3}{10}$$

3.451. *¿Qué probabilidad hay de conseguir un número que empiece por 3, de todos los de seis cifras que se pueden formar con los guarismos 3, 3, 3, 5, 0, 0?*

Casos posibles: número de números de seis cifras

$$PR_6^{3,2} - PR_5^3 = 40$$

Casos favorables: de esos cuarenta, empiezan por 3

$$PR_5^{2,2} = 30$$
$$p = 3/4$$

3.452. *De una baraja de cuarenta naipes se extrae un paquete de cinco cartas. ¿Qué probabilidad hay de que ese paquete contenga dos ases?; y, ¿cuál de que ese grupo de cinco cartas, tenga, al menos, dos ases?*

A) *Casos favorables*: hay todas estas maneras de obtener dos ases: $\binom{4}{2}$; por cada manera de ésas, los dos ases pueden estar acompañados de tres cartas no ases de todos estos modos: $\binom{36}{3}$.

Luego todos los casos favorables de obtener un par de ases son

$$\binom{4}{2} \quad \binom{36}{3}$$

Casos posibles: todos los posibles paquetes de cinco cartas con los cuarenta naipes de la baraja son $\binom{40}{5}$

$$p = \frac{\binom{4}{2} \cdot \binom{36}{3}}{\binom{40}{5}}$$

B) El suceso H = «obtener al menos dos ases» tiene por suceso contrario $\bar{H}$ = «obtener cero ases o un as»; es decir:

$$\bar{H} = H_0 \cup H_1$$

$$p(H) = 1 - p(\bar{H}) = 1 - p(H_0 \cup H_1) = 1 - p(H_0) - p(H_1)$$

$$p(H) = 1 - \frac{\binom{36}{5} + \binom{4}{1} \cdot \binom{36}{4}}{\binom{40}{5}}$$

También se podía haber resuelto mediante la reunión triple

$$H = H_2 \cup H_3 \cup H_4$$

3.453. ***Se dispone de dos cajas iguales, contenedoras de dos bolas blancas, tres rojas y cuatro negras, la primera, y de tres blancas, cuatro rojas y cinco negras, la segunda. Se toma, al azar, una bola de cada una de las cajas. ¿Qué probabilidad hay de que se hayan conseguido del mismo color?***

El suceso H = «obtener par isocromo» puede producirse, si se verifica uno de estos tres:

$$\left.\begin{array}{l} B = \text{«obtener par blanco»} \\ R = \text{«obtener par rojo»} \\ N = \text{«obtener par negro»} \end{array}\right\} H = B \cup R \cup N$$

Los sucesos B, R y N son incompatibles (*i*).

De otro lado, para que se produzca el suceso B, han de realizarse los sucesos

b_1 = «obtener bola blanca de la primera caja» y
b_2 = «obtener bola blanca de la segunda caja», de modo que
$B = b_1 \cap b_2$;

de igual manera,

$$R = r_1 \cap r_2;$$
$$N = n_1 \cap n_2$$

Los sucesos b_1 y b_2, r_1 y r_2, n_1 y n_2 son sucesos independientes (*ii*).
Componiendo ahora el análisis que se ha hecho del suceso H, resulta:

$$H = (b_1 \cap b_2) \cup (r_1 \cap r_2) \cup (n_1 \cap n_2).$$

La probabilidad pedida, teniendo en cuenta las observaciones (*i*) e (*ii*) es

$$p(H) = p(b_1) \cdot p(b_2) + p(r_1) \cdot p(r_2) + p(n_1) \cdot p(n_2)$$
$$p(H) = \frac{2}{9} \cdot \frac{3}{12} + \frac{3}{9} \cdot \frac{4}{12} + \frac{4}{9} \cdot \frac{5}{12} = \frac{19}{54}$$

3.454. ***Se lanza al aire una moneda trucada diez veces consecutivas, de modo que la probabilidad de obtener «cara», cada vez es 3/4. ¿Qué probabilidad hay de obtener, al menos, una vez cruz?***

H = «obtener, al menos, una vez cruz»
$\bar{H}$ = «obtener siempre cara»
$\bar{H} = c_1 \cap c_2 \ldots \cap c_{10}$

Los sucesos $c_1, c_2, \ldots c_{10}$ son independientes, de modo que

$$p(\bar{H}) = \frac{3}{4} \cdot \frac{3}{4} \cdot \ldots \text{(10 veces)}$$

$$p(H) = 1 - \left(\frac{3}{4}\right)^{10}$$

3.455. *Se propone a un equipo de tres alumnos la resolución de un problema. Se estima, en función de sus evaluaciones, que la probabilidad de que lo resuelva el primero es 1/2; la de que lo haga el segundo, 1/3 y 1/4 la probabilidad de que lo consiga resolver el tercero. ¿Cuál es la probabilidad de que resuelva el problema el equipo?*

Siendo A, B y C los sucesos de resolución para cada uno de los alumnos, el suceso H cuya probabilidad se pide es $H = A \cup B \cup C$.

Como A, B y C son sucesos compatibles, el teorema de la probabilidad total, para tres sucesos, resuelve la cuestión:

$$p(H) = p(A) + p(B) + p(C) - p(A \cap B) - p(A \cap C) - p(B \cap C) + p(A \cap B \cap C)$$

$$p(H) = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{2} \cdot \frac{1}{3} - \frac{1}{2} \cdot \frac{1}{4} - \frac{1}{3} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{4} = \frac{3}{4}$$

Adviértase que A, B y C son sucesos independientes.

3.456. *Tres jugadores, A, B y C, lanzan una moneda homogénea, al aire, en ese orden, continuando el juego hasta que uno de ellos consiga obtener cruz. ¿Cuál es la probabilidad de ganar que tiene cada uno de los tres jugadores?*

Analicemos el suceso A = «sacar cruz el primero».

En principio, puede ganar en la primera tirada o en la segunda o en la tercera o en la n-sima, de modo que

$$A = A_1 \cup A_2 \cup \ldots \cup A_n$$

Pero para que se pueda verificar A_2, es necesario que en la primera tirada hayan fallado A, B y C, de modo que el suceso A_2 está formado por la intersección cuádruple

$$A_2 = \bar{a}_1 \cap \bar{b}_1 \cap \bar{c}_1 \cap a_2.$$

Si es en la tercera tirada, A_3, donde gana el primero, análogamente

$$A_3 = \bar{a}_1 \cap \bar{b}_1 \cap \bar{c}_1 \cap \bar{a}_2 \cap \bar{b}_2 \cap \bar{c}_2 \cap a_3$$

El proceso se repite hasta la n-sima tirada, lo que supone para el suceso A la siguiente composición:

$$A = a_1 \cup (\bar{a}_1 \cap \bar{b}_1 \cap \bar{c}_1 \cap a_2) \cup (\bar{a}_1 \cap \bar{b}_1 \cap \bar{c}_1 \cap \bar{a}_2 \cap \bar{b}_2 \cap \bar{c}_2 \cap a_3) \cup \ldots$$

Los reunidos son incompatibles y los intersecados independientes, de manera que

$$p(A) = p(a_1) + p(a_1) \cdot p(b_1) \cdot p(c_1) \cdot p(a_2) + \ldots$$
$$p(A) = 1/2 + (1/2)^4 + (1/2)^7 + \ldots$$

Se trata de la suma de los términos de una progresión geométrica, ilimitada, decreciente, de razón 1/8. El límite de esa suma proporciona la probabilidad buscada:

$$p(A) = \frac{1/2}{1 - 1/8} = \frac{4}{7}$$

Del mismo modo se calculan las probabilidades de ganar de los otros dos jugadores, que son

$$p(B) = \frac{2}{7}$$

$$p(C) = \frac{1}{7}$$

3.457. ***A y B establecen el siguiente juego, sobre una baraja de cuarenta cartas: si al extraer un naipe, resulta ser figura o as, gana A, perdiendo en todos los demás casos de extracción. ¿Cuáles deberán ser las apuestas o posturas de A y de B para que el juego sea equitativo?***

En juegos de azar, se denomina esperanza matemática de un jugador al producto del premio por la probabilidad de obtenerlo. Y un juego es equitativo, si las puestas de los jugadores coinciden con sus esperanzas matemáticas.

$$\left.\begin{array}{l} P(A) = \text{premio} \times p_A = \text{premio} \times 16/40 \\ P(B) = \text{premio} \times p_B = \text{premio} \times 24/40 \end{array}\right\} \frac{P(A)}{P(B)} = \frac{2}{3}$$

3.458. ***Se tienen en una urna 100 bolas blancas, 200 negras y 300 verdes. ¿Qué probabilidad hay de sacar en tres ensayos, con remplazamiento, una bola de cada color? Y, ¿cuál sin remplazamiento?***

A) *Con remplazamiento* (volviendo a introducir la bola)

Conseguir la secuencia $b - n - v$, es un suceso formado por la intersección de tres independientes, de modo que su probabilidad es el producto de las de sus componentes

$$\frac{100}{600} \cdot \frac{200}{600} \cdot \frac{300}{600} = 1/36$$

Como el suceso pedido se verifica cuando lo hacen cualquiera de las P_3 secuencias a que da lugar la considerada, y el conseguir una u otra de esas secuencias son sucesos incompatibles, la probabilidad buscada es la suma de $P_3 = 6$ sumandos iguales:

$$p = P_3 \cdot 1/36 = 1/6$$

B) *Sin remplazamiento*

Analícese que el resultado es $P_3 \cdot \frac{100}{600} \cdot \frac{200}{599} \cdot \frac{300}{598}$

3.459. *Un trirreactor tiene como coeficientes de seguridad, intrínsecos, para sus motores, 0,99 para el central y 0,97 para cada uno de sus dos laterales. El avión puede maniobrar con sus tres motores, sólo con el central o con los dos laterales, abatiéndose a tierra en los demás casos. ¿Qué probabilidad hay de que llegue a destino?*

El suceso H = «llegar a destino» se puede verificar de estos tres modos incompatibles:

A = «con los tres motores»
B = «con los dos laterales»
C = «con el central»

$$H = A \cup B \cup C$$

A su vez, los sucesos A, B y C están formados por la intersección de los sucesos independientes que se indican (denotamos I a los laterales y Φ al central)

$$A = I \cap \Phi \cap I$$
$$B = I \cap \bar{\Phi} \cap I$$
$$C = \bar{I} \cap \Phi \cap \bar{I}$$

Resulta entonces, que la probabilidad pedida es

$$p(H) = p^2(I) \cdot p(\Phi) + p^2(I) \cdot p(\Phi) + p^2(\bar{I}) \cdot p(\Phi) = 0{,}94$$

3.46. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

3.460.
En una urna hay cincuenta bolas numeradas con los cincuenta primeros números naturales. ¿Qué probabilidad hay de sacar las cincuenta bolas en el orden natural?

3.461.
¿Cuál es la probabilidad de obtener «de mano» póker de reyes, de una baraja de cincuenta y dos cartas?

3.462.
Al destapar una pieza de dominó, ¿qué probabilidad existe de conseguir una suma de puntos múltiplo de 4?; ¿y múltiplo de 6?

3.463.
Se lanzan nueve monedas al aire. ¿Qué probabilidad hay de conseguir cinco caras y cuatro cruces?

3.464.

¿Qué probabilidad existe de obtener, de mano, «full de ases»?

NOTA. La jugada «full de ases» la constituyen tres ases y una pareja (=dos cartas iguales).

3.465.

¿Cuál es la probabilidad de que lanzando tres dados se obtengan nueve puntos?; ¿cuál la de obtener diez?

3.466.

En una bolsa hay b bolas blancas y n negras. Un operador extrae k bolas. ¿Cuál es la probabilidad de que resulten i blancas y $k - i$ negras?

3.467.

¿Cuál es la probabilidad de que al lanzar dos dados n veces, se obtenga, al menos, un seis doble?

¿Cuántas tiradas habrían de realizarse para que esa probabilidad llegara a valer 0,5?

3.468.

¿Cuál es la probabilidad de torpedear un barco, sabiendo que sólo pueden lanzarse tres torpedos y que la probabilidad de hacer blanco en cada uno de los disparos es 0,25?

3.469.

La probabilidad de un suceso A es 0,1. Calcúlese la probabilidad de que el suceso se verifique al menos cien veces en mil pruebas.

NOTA. Tal vez fuera bueno abordar este problema tras el estudio de las distribuciones binomiales, en el próximo capítulo.

3.5

Estadística

3.51. Introducción. Definición. Partes. Objetivos

3.52. Estadística descriptiva; distribuciones monovariantes

3.521. *Terminología. Caracteres estadísticos. Muestra y población*
3.522. *Variables cualitativas. Tablas y gráficos*
3.523. *Variables cuantitativas. Tablas y gráficos*

3.5231. Variación discreta
3.5232. Variación continua

3.524. *Reducción de la información: estadísticos*

3.5241. Estadísticos de centralización
3.5242. Estadísticos de dispersión
3.5243. Estadísticos de asimetría. Momentos centrales

3.53. Estadística descriptiva; distribuciones bivariantes

3.531. *Dependencia funcional y aleatoria: variables estadísticas bidimensionales*
3.532. *Tablas y gráficos*
3.533. *Regresión. Regresión lineal*
3.534. *Ajuste. Método de los mínimos cuadráticos*
3.535. *Cálculo abreviado de las rectas de regresión*
3.536. *Reducción de la información: estadísticos bivariantes. Correlación*

3.54. Distribuciones y poblaciones aleatorias

3.541. *Introducción*
3.542. *Distribuciones aleatorias: función de distribución y función de densidad*
3.543. *Momentos de una distribución*
3.544. *Distribución binomial*
3.545. *Distribución normal*

3.5451. Establecimientos
3.5452. Tipificación de la variable. Tablas z/A

3.546. *La distribución normal como aproximación de la binomial. Corrección de Yates*
3.547. *Distribución de Poisson*

3.55. Estadística inferencial

3.551. *Concepto. Clasificación*
3.552. *Estadística inferencial inductiva*
3.553. *Estadística inferencial hipotético-deductiva*

3.56. Aplicabilidad. Automatismos y destrezas

3.5

Estadística

3.51. INTRODUCCION. DEFINICION. PARTES. OBJETIVOS

La génesis de la Estadística se pierde en la más remota antigüedad. Se tienen noticias históricas de *censos* chinos del siglo XXIII a. de C. Tampoco cabe ninguna duda de que los egipcios tabulaban sus riquezas y potencial humano, antes del éxodo hebreo. Tácito, con su ajustada prosa de historiador sobrio, relata la orden de César Augusto, referente a censar sus ejércitos, marina, tesoros y habitantes de su imperio.

Hacia 1650 aparece por primera vez en Centroeuropa la palabra «Estadística», para indicar el conjunto de métodos de recolección de datos y documentación útil en la administración del Estado (*status*).

Junto a esta línea, procedente de la exigencia del gobernante, para conocer su gobierno y realizar su administración, paralelamente a ella se desarrolla otra vía de evolución de esta ciencia, y con una causa bien distinta y hasta trivial, en su raíz: los juegos de azar. Durante los siglos XVII y XVIII, en las sofisticadas cortes europeas —principalmente en Francia— el juego se pone de moda, y grandes matemáticos, como Pascal y Fermat, en París, o De Moivre —después— exiliado en Londres, al servicio de los aristócratas, dan un tremendo impulso a la Estadística y cálculo de probabilidades, al intentar resolver los problemas de juego que sus acaudalados clientes les proponían.

A partir de entonces, la exigencia que la sociedad hace continuamente a la Matemática para poder avanzar en el estudio de la Sociología, Psicología, Biología, Genética, Economía, Política y tantas otras disciplinas, han provocado un enorme crecimiento de la ciencia estadística.

Siguiendo al profesor S. Ríos, se puede anunciar en general:

Estadística es la ciencia que proporciona los métodos para el tratamiento de

las masas de datos de observación, para decidir la afirmación o rechazo de ciertas afirmaciones o leyes.

Conviene establecer claramente las partes de la Estadística, bien distintas en sus pretensiones e instrumentos de cálculo. Intentaremos avanzar aquí una panorámica del conjunto, indicando sus objetivos, servidumbres e interconexiones.

Estadística descriptiva: Se encarga esta parte de la Estadística de

— recoger datos,
— coleccionar datos,
— representar datos y,
— tratar la información, reduciendo a «estadísticos».

Le basta, como instrumento, el cálculo elemental.

Estadística inferencial: Tiene por objeto

— desarrollar las técnicas necesarias para calcular o comprobar los *parámetros* de una población, a partir de los datos suministrados por la Estadística descriptiva de un subconjunto de la población, representativo y aleatorio, llamado muestra;
— medir la incertidumbre de las conclusiones, en términos de probabilidad.

Como se verá en su epígrafe correspondiente, la Estadística inferencial, a su vez, tiene dos partes, tituladas *Estadística inferencial inductiva* y *Estadística inferencial hipotético-deductiva*, encargadas de resolver los específicos problemas de sus ámbitos que allí se describen.

La Estadística inferencial también suele llamarse *teoría de muestras*.

El problema de la toma de muestras, para la inferencia estadística, no corresponde propiamente a la Estadística, sino que ha de venir resuelto por una disciplina anexa a ella, que se denomina *diseño de experimentos*.

De un modo simplista, como corresponde a inicio de capítulo, se esquematiza lo dicho en el cuadro de la página siguiente*.

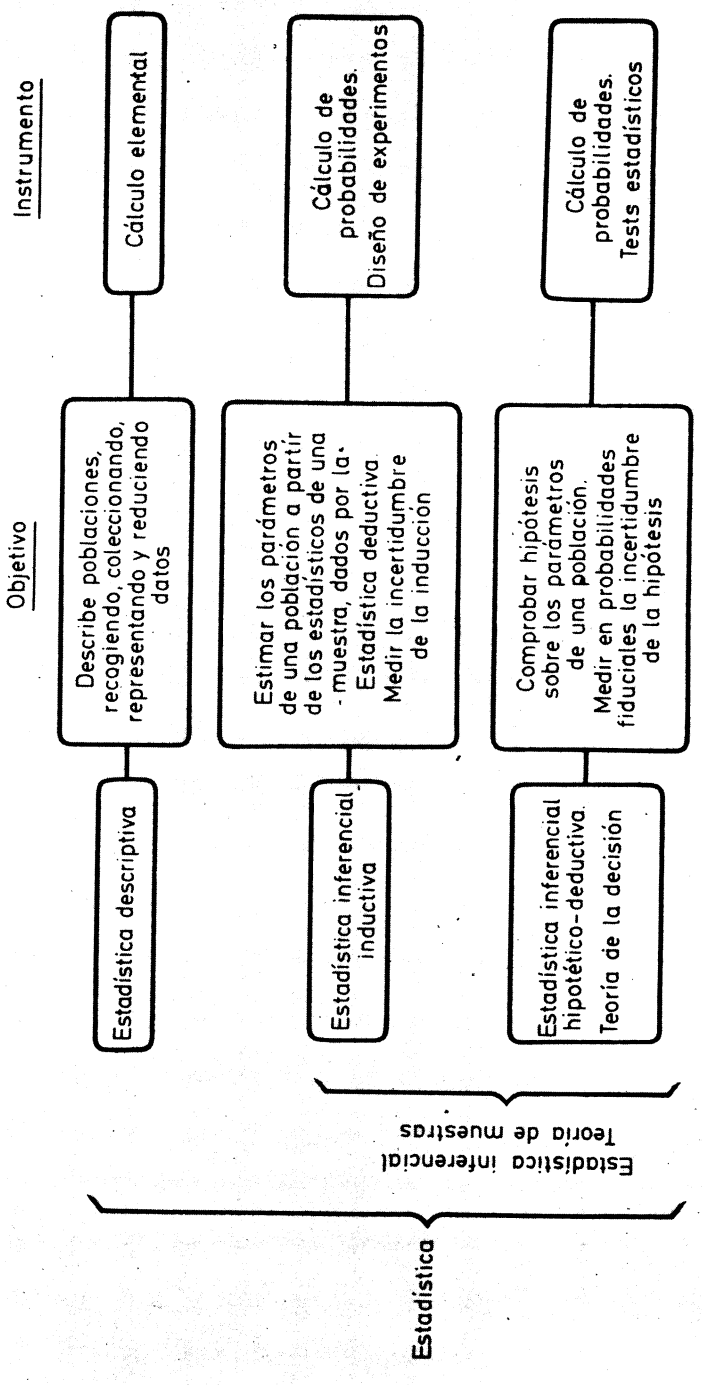
3.52. ESTADISTICA DESCRIPTIVA; DISTRIBUCIONES MONOVARIANTES

3.521. Terminología. Caracteres estadísticos. Muestra y población

Se denomina *variable aleatoria o estadística* a la variable que toma «valores», llamados *resultados*, dentro de un determinado dominio o *carácter*, con una determinada frecuencia o probabilidad.

La variable aleatoria puede ser *cualitativa* o *cuantitativa*. En el primer caso, los resultados que pueden aparecer en su carácter o *atributo* suelen llamarse *modalidades* o *rúbricas*. Si son dos las modalidades cualitativas que cubren el conjunto

* Claro está que el fruto del cuadro se sacará completo al término del estudio del presente capítulo.


Estadística
Estadística inferencial
Teoría de muestras
Estadística descriptiva
Estadística inferencial inductiva
Estadística inferencial hipotético-deductiva.
Teoría de la decisión
Objetivo
Describe poblaciones, recogiendo, coleccionando, representando y reduciendo datos
Estimar los parámetros de una población a partir de los estadísticos de una muestra, dados por la Estadística deductiva. Medir la incertidumbre de la inducción
Comprobar hipótesis sobre los parámetros de una población. Medir en probabilidades fiduciales la incertidumbre de la hipótesis
Instrumento
Cálculo elemental
Cálculo de probabilidades. Diseño de experimentos
Cálculo de probabilidades. Tests estadísticos

de resultados, la variable se llama *dicotómica* y, por extensión, el carácter se denomina dicotómico.

A su vez, una variable aleatoria cuantitativa puede ser *discreta* o *continua*, según que pueda tomar solamente determinados valores o todos los innumerables de su dominio. Si la variación cuantitativa discreta o discontinua se lleva a cabo de unidad en unidad, se dice entonces que se trata de un carácter aleatorio *merístico*.

Ejemplo 1

La variable aleatoria «borde de las hojas» sobre un conjunto de guisantes es una variable cualitativa sobre un carácter dicotómico, pues sus dos únicas modalidades son «hoja dentada» y «hoja lisa».

Ejemplo 2

La variable aleatoria «número de puntos obtenidos al lanzar un dado» es una variable con carácter cuantitativo discreto, ya que no se pueden dar todos los innumerables resultados reales del intervalo de variación 1-6.

Ejemplo 3

La variable estadística «espesor de dieléctrico» de una fabricación en serie de una determinada pieza de un condensador es una variable aleatoria cuantitativa continua, pues, teóricamente, puede tomar cualquier valor del intervalo de extremos mayor y menor espesores conseguidos.

Ejemplo 4

Un ejemplo de variable aleatoria cuantitativa discreta de carácter merístico es «número de hijos de todas las familias de un cónclave humano», ya que la variación se produce de unidad en unidad.

Población y muestra

Se denomina *población* al conjunto de individuos que poseen el carácter aleatorio, objeto del estudio estadístico.

Muy frecuentemente, por extensión, recibe el nombre de población no el conjunto de individuos, sino el propio conjunto de resultados, obtenidos de ellos, referibles al carácter estudiado.

Las poblaciones pueden ser finitas o infinitas.

Se llama *muestra* todo subconjunto de la población, que se aísla para su análisis estadístico.

La mayor parte de las veces, la Estadística descriptiva trabaja con muestras que —como se verá— han de ser *aleatorias* y *representativas* de la población. Son claras las razones de ello: bien porque se trate de poblaciones realmente infinitas, que prohíban absolutamente su estudio completo, bien porque sean poblaciones muy grandes, prácticamente inabordables en su totalidad, o bien porque las experiencias a realizar sean destructivas, el estudio se realiza sobre muestras y no sobre poblaciones.

Ejemplo

Sobre el conjunto de todos los ciudadanos de un país A, se considera la variable estadística «renta per cápita».

Siendo muy difícil tomar todos los datos de la población, se ha de aislar un subconjunto de ella, una muestra aleatoria y representativa (tarea nada fácil).

3.522. Variables cualitativas. Tablas y gráficos

Tanto en el tratamiento de las variables estadísticas cualitativas como cuantitativas, como ya queeó dicho, la Estadística descriptiva procede, lo primero, a la recolección de datos.

Son multitud los procedimientos y técnicas para llevarla a cabo y de muy diversa índole, según el campo del estudio estadístico: desde las encuestas directas hasta el uso de las computadoras, pasando por las series de experimentos realizados por el investigador en ciencias positivas, como la Física, Química o Biología.

En cualquier caso, la recolección de datos es un problema delicado, pues un error en esta fase falsea todo el tratamiento posterior; de ahí que, una vez concluida, haya de hacerse un detenido escrutinio de los números conseguidos, a fin de revisar datos sospechosos o rechazar los claramente inadmisibles.

Una vez en disposición de los datos, la segunda tarea que aborda la Estadística descriptiva es la de coleccionar o tabular esos datos, y un tercer trabajo consiste en representar esos números «censados» en adecuados gráficos de comprensión inmediata.

A continuación se desarrollan estos procesos, para variables cualitativas.

Sea una población de N individuos, descrita según un atributo X, cuyos resultados son las siguientes k modalidades:

$$X = \{x_1, x_2, \ldots x_k\}$$

Denotando por n_1 la frecuencia absoluta con que se presenta la modalidad x_i y por h_i la frecuencia relativa de la misma rúbrica del atributo, es claro que

$$\sum_{i=1}^{k} n_i = N; \text{ y que } \sum_{i=1}^{k} h_i = \sum_{i=1}^{k} \frac{n_i}{N} = 1$$

La tabla de frecuencias se dispone del siguiente modo:

X	n_i	h_i
x_1	n_1	h_1
x_2	n_2	h_2
.	.	.
.	.	.
x_k	n_k	k_k
	$\Sigma n_i = N$	$\Sigma h_i = 1$

Ejemplo

Ocupaciones predominantes de la población activa femenina. España, 1960. (Fuente: Bases para una política educativa. M. E. C.)

Ocupaciones (X)	*Cifras absolutas* (n_i)	*Frecuencias* (h_i)
Servicio doméstico	577 571	0,338
Sector agrícola	409 580	0,237
Artesanas y jornaleras	422 096	0,246
Comercio	54 583	0,032
Empleadas en la Administración	119 573	0,070
Profesión técnica	114 387	0,067
	$\Sigma n_i = 1\,697\,790$	$\Sigma h_i = 1$

Para presentar las distribuciones de frecuencias de estas variables estadísticas cualitativas, pueden utilizarse los *diagramas de barras*, los *ciclogramas* o gráficos de sectores o los *pictogramas*.

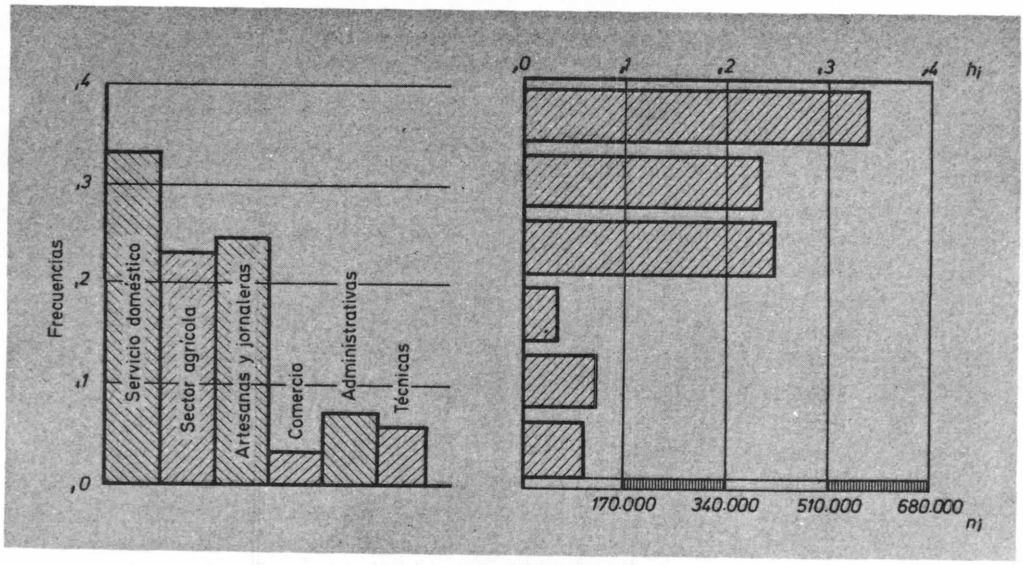
Los primeros, que se pueden disponer vertical u horizontalmente, se construyen dibujando unos rectángulos de bases convencionales (disposición vertical) y cuyas alturas son proporcionales a las frecuencias absolutas y relativas de cada una de las modalidades que toma el atributo.

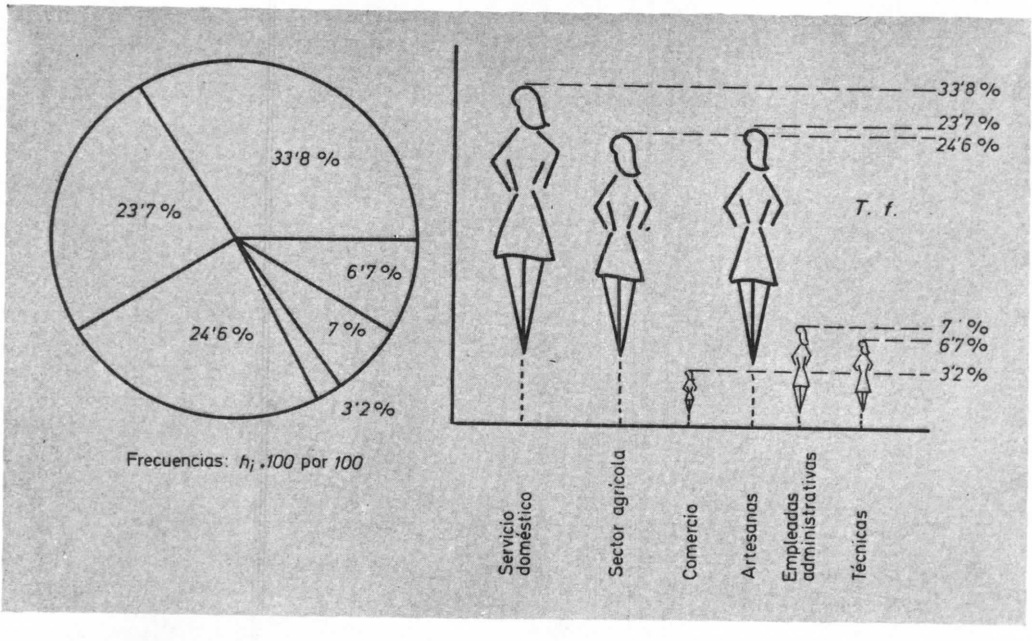
Los ciclogramas se construyen sobre un círculo o semicírculo, disponiendo sectores cuyas amplitudes angulares son proporcionales a las frecuencias de cada una de las rúbricas o modalidades del atributo.

Los pictogramas son una variante de los diagramas de barras. En ellos, en lugar de la abstracción geométrica de los rectángulos, se dibujan filas o columnas de individuos alusivos a la composición de la población. Así, si se tratara de una distribución de rentas, podrían utilizarse columnas de monedas, de diferente altura según la frecuencia de cada modalidad representada. En el ejemplo que hemos dispuesto, filas de mujeres, en silueta, de mayor o menor longitud, constituyen el pictograma de la distribución planteada, referente al empleo femenino.

Dibujamos los diagramas del ejemplo utilizado, lo que nos libera de cualquiera otra descripción (ver gráficos de la página siguiente).

Otras representaciones gráficas de estas variables estadísticas cualitativas son los *cartogramas*. Resultan muy adecuados cuando el atributo es referible a individuos cuya esencia es que integran sintópicamente la población; tal sucede con el ejemplo que se inserta a continuación: el carácter «matrícula universitaria» se plasma sobre las provincias españolas, según su frecuencia, en diferentes colores, fondos o rayados.

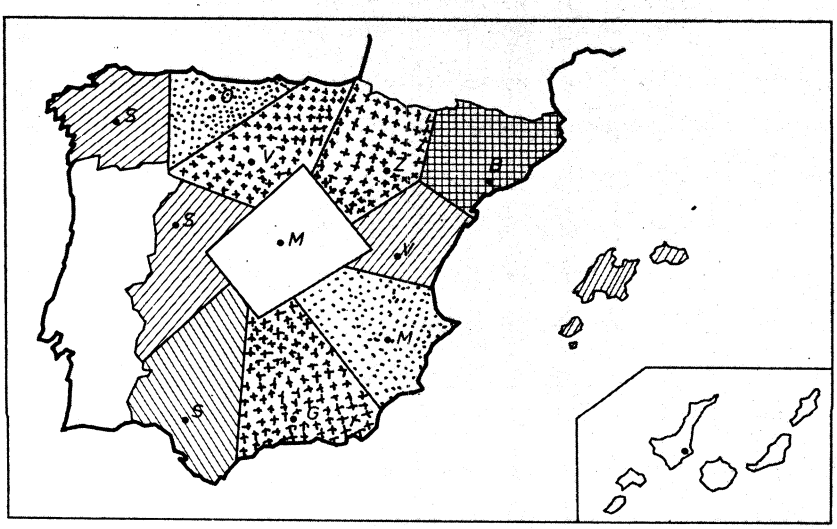

Frecuencias
,4
,3
,2
,1
,0
Servicio doméstico
Sector agrícola
Artesanas y jornaleras
Comercio
Administrativas
Técnicas
,0
,1
,2
,3
,4
hi
170.000
340.000
510.000
680.000
ni


33'8 %
23'7 %
6'7 %
24'6 %
7 %
3'2 %
Frecuencias: hi ,100 por 100
33'8 %
23'7 %
24'6 %
T. f.
7 %
6'7 %
3'2 %
Servicio doméstico
Sector agrícola
Comercio
Artesanas
Empleadas administrativas
Técnicas

Ejemplo

Matrícula universitaria, por distritos. Curso 1966-67.
(Fuente: Secretaría General Técnica del M.E.C.)
(No se incluyen las universidades no estatales.)

Distrito (X)	(n_i)	*Matrícula* (h_i)	($h_i \cdot 100\ \%$)
Barcelona	13 665	0,136	13,6
Granada	8 492	0,084	8,4
La Laguna	1 423	0,014	1,4
Madrid	35 975	0,356	35,6
Murcia	2 088	0,020	2,0
Oviedo	3 139	0,032	3,2
Salamanca	5 780	0,057	5,7
Santiago	5 004	0,049	4,9
Sevilla	5 886	0,058	5,8
Valencia	5 967	0,059	5,9
Valladolid	7 126	0,070	7,0
Zaragoza	6 580	0,065	6,5
	$\Sigma n_i = 101\ 125$	$\Sigma h_i = 1$	$\Sigma h_i \cdot 100 = 100$



$h_i > 35\ \%$

$35\ \% > h_i > 15\ \%$

$8{,}5\ \% > h_i \geq 6{,}5\ \%$

$4{,}5\ \% < h_i < 6\ \%$

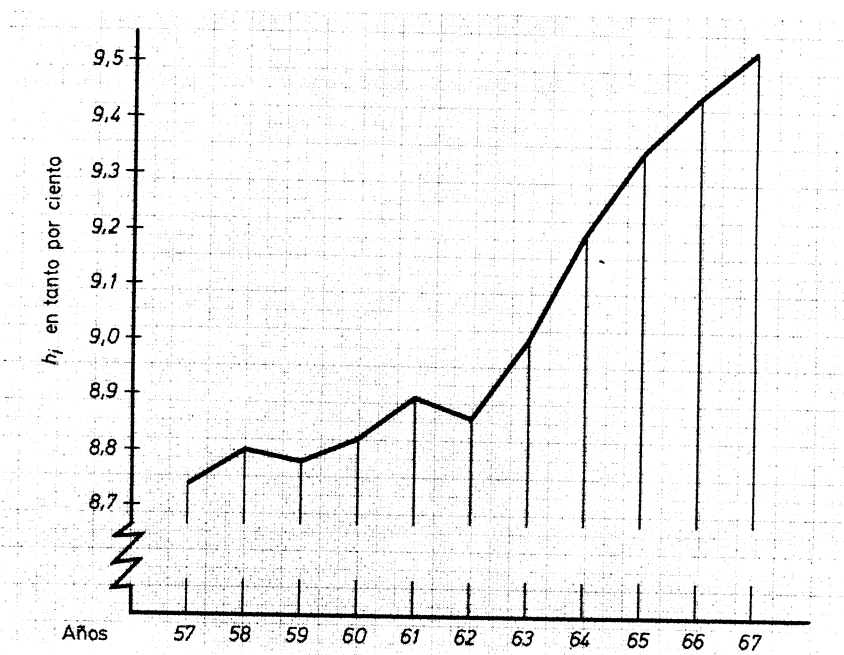
$h_i < 4{,}5\ \%$

Finalmente, para terminar este epígrafe, hagamos referencia a las llamadas *series cronológicas*, que son distribuciones de frecuencias de una variable estadística cualitativa cuyo atributo es, precisamente, el tiempo-calendario, y sus diversas rúbricas o modalidades son los años-fecha. El ejemplo que se dispone a continuación es una serie cronológica.

Ejemplo.

Crecimiento de la población española en edad de escolaridad obligatoria. (Fuente: I.N.E.)

Año (X)	*Población de seis a trece años* (n_i)	(h_i)
1957	4 242 321	0,0874
1958	4 266 734	0,0880
1959	4 265 562	0,0878
1960	4 287 821	0,0883
1961	4 315 891	0,0890
1962	4 300 500	0,0886
1963	4 356 957	0,0900
1964	4 449 372	0,0920
1965	4 534 297	0,0934
1966	4 584 972	0,0945
1967	4 624 959	0,0953
	$\Sigma n_i = 48\,529\,386$	$\Sigma h_i = \sim 1$



3.523. Variables cuantitativas. Tablas y gráficos

3.5231. *Variación discreta*

Las tablas de distribución de frecuencias para una variable estadística cuantitativa discreta en nada se diferencian de la forma típica de las de variables cualitativas (pág. 388), excepto en que aquí, tratándose de una variable cuantitativa, la columna de las x_i estará ocupada, en lugar de con los nombres de las diversas rúbricas del atributo, con los valores numéricos que tome la variable.

Por lo que se refiere a la representación, la más adecuada para este caso es un diagrama de ordenadas o de barras, pudiéndose usar también los llamados diagramas de puntos.

El ejemplo que a continuación se dispone concreta lo que se viene diciendo y nos libera de más amplias descripciones.

Ejemplo

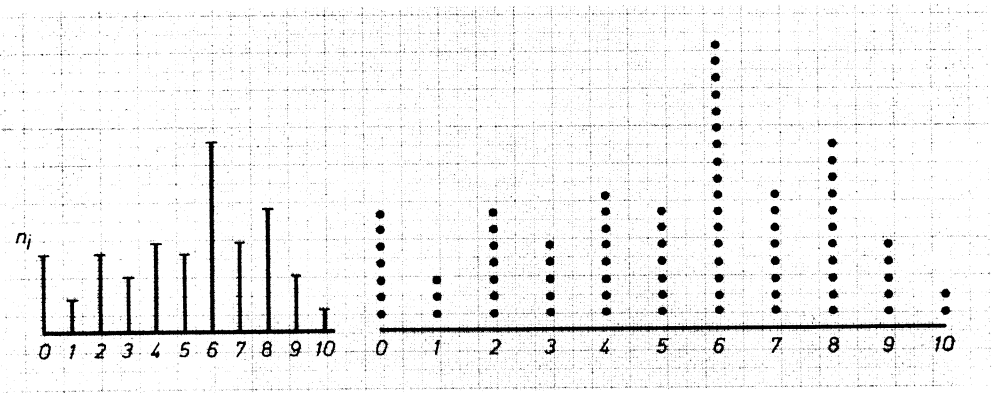
Asignando 1 punto a cada uno de los 10 ítems de una prueba objetiva, realizada por 80 alumnos, las calificaciones obtenidas han sido las siguientes:

0	3	7	4	6	3	5	6	0	7	2	0	5	8	9	6
3	10	7	4	3	8	0	4	8	0	2	10	2	7	8	1
4	8	9	8	8	5	6	6	4	0	6	0	6	6	6	7
8	6	3	5	6	1	8	2	8	6	5	4	2	7	7	2
9	6	6	9	7	2	6	9	6	5	8	4	6	1	4	5

La tabla de frecuencias, que incluye el contaje o recuento de las mismas es:

Calificación (X_i)	*Recuento*	n_i	h_i
0	𝍸 //	7	0,087
1	///	3	0,038
2	𝍸 //	7	0,087
3	𝍸	5	0,062
4	𝍸 ///	8	0,100
5	𝍸 //	7	0,087
6	𝍸 𝍸 𝍸 //	17	0,215
7	𝍸 ///	8	0,100
8	𝍸 𝍸 /	11	0,137
9	𝍸	5	0,062
10	//	2	0,025
		$\Sigma n_i = 80$	$\Sigma h_i = 1$

He aquí sus diagramas de ordenadas y de puntos:



3.5232. *Variación continua*

El caso más frecuente, y más interesante, es cuando la variable estadística cuantitativa presenta una variación continua, a lo largo de su intervalo de valores.

En estos casos existen dos maneras de construir las tablas de distribución de frecuencias:

— método simple,
— método de las frecuencias agrupadas.

Método simple. En todo similar al tratamiento que se ha dado a las variables estadísticas cuantitativas discretas, resulta su tabla de disposición idéntica a las de éstas.

En cuanto a sus representaciones gráficas, junto a los diagramas de barras o de puntos, ya expuestos, resulta interesante en este caso, la construcción del llamado *diagrama acumulativo.* Se dibuja a partir del diagrama de puntos, acumulando a cada ordenada todas las frecuencias anteriores.

Ejemplo

El departamento de verificación de una factoría de aparatos eléctricos toma, para control de calidad, cien piezas de un determinado diseño y mide su espesor en milímetros, habiendo resultado los siguientes números:

1,80	1,90	1,93	2,02	2,01	2,00	2,03	2,04	2,08	1,93
1,83	1,91	1,95	1,93	1,99	2,00	2,00	2,07	2,04	2,08
1,83	1,92	1,96	1,95	1,99	1,99	1,98	2,04	2,05	2,09
1,84	1,90	1,95	1,96	2,00	2,02	1,98	2,04	2,07	2,09
1,83	1,92	1,93	1,95	2,01	2,02	2,01	2,05	2,06	2,10
1,86	1,89	1,97	1,93	2,00	2,01	1,98	2,07	2,05	2,11
1,88	1,88	1,97	1,97	2,01	1,99	1,98	2,06	2,06	2,11
1,89	1,93	1,94	1,98	1,99	2,02	1,99	2,05	2,08	2,18
1,91	1,97	1,95	2,02	1,98	1,98	2,02	2,06	2,12	2,22
1,92	1,94	1,96	1,98	2,00	2,01	2,00	2,03	2,12	2,27

El diagrama acumulativo de esta distribución de frecuencias es el de la página siguiente.

Método de frecuencias agrupadas. Cuando, como en el ejemplo que antecede, el número de valores que toma la variable es elevado, se usa el método de frecuencias agrupadas, cuya técnica se describe a continuación, usando el mismo ejemplo precedente.

1.° Se determina el intervalo total de variación

$$\left.\begin{array}{l}\text{espesor máximo} = 2{,}27 \text{ mm} \\ \text{espesor mínimo} = 1{,}80 \text{ mm}\end{array}\right\} 2{,}27 - 1{,}80 = 0{,}47 \text{ mm}$$

2.° Se divide este intervalo total en tantas *clases* como se quiera describir la distribución de frecuencias. No existe número idóneo, aunque conviene evitar los extremos: un número pequeño de clases «diluiría» las diferencias y perdería «finura» la distribución; optar por un número excesivamente grande de clases desvirtuaría el método, ya que con él se pretende una simplicación de cálculos. Puede aconsejarse un número discreto entre diez y veinte clases.

$$0{,}47 : 10 = 0{,}047 \text{ mm}$$

Es obvia la conveniencia de «redondear» el *intervalo de clase* a un número más «operativo»: 0,05 mm.

3.° Es necesario delimitar muy claramente los extremos de cada una de las clases (también llamadas «casillas»), a fin de que no haya ninguna duda al asignar cada dato a su clase correspondiente. Hay dos técnicas para conseguirlo: bien se especifican los extremos de cada intervalo con una cifra más de las que dan las observaciones, bien se utilizan los signos $\leq$ y $<$ que abren y cierran, respectivamente, cada intervalo.
En el ejemplo que se viene desarrollando, la primera clase, siendo la mínima observación 1,80 mm, tendrá como extremos

$$1{,}775 - 1{,}825$$

ò bien

$$1{,}77 \leq x_1 < 1{,}82$$

4.° Una vez establecidas las clases (las diez de nuestro ejemplo) han de establecerse las *marcas de clase* de cada una de ellas, que es el valor común que se le asigna a todos los datos comprendidos en la clase correspondiente. Es lógico que su cálculo se haga con la semisuma de extremos.
Así, la marca de clase de x_1 es

$$\frac{1{,}775 + 1{,}825}{2} = 1{,}80$$

5.° Con los cálculos precedentes se construye la tabla de la distribución de frecuencias agrupadas, cuyas siete columnas se describen por sí solas, sobre el ejemplo que se desarrolla.

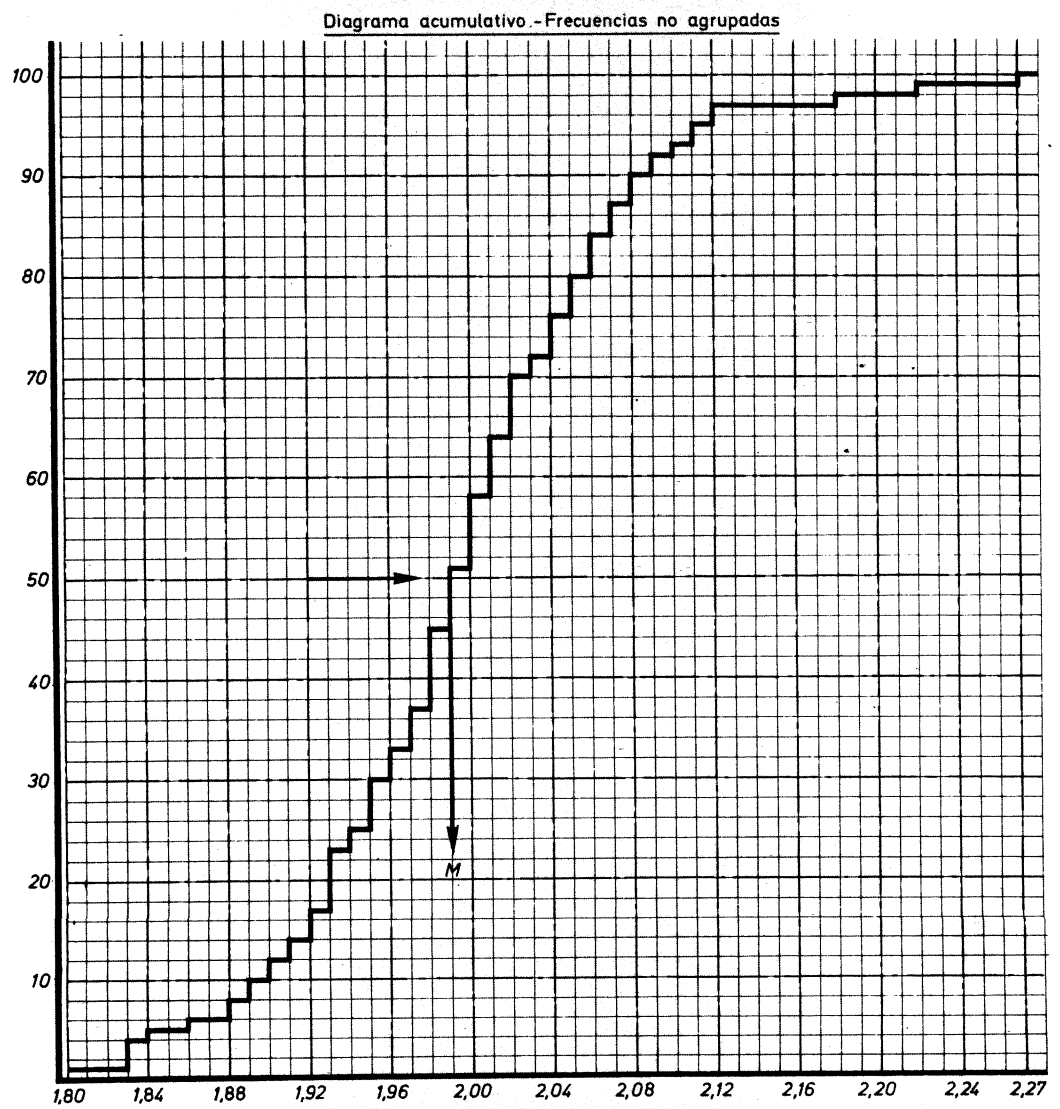


Diagrama acumulativo.-Frecuencias no agrupadas
100
90
80
70
60
50
40
30
20
10
M
1,80
1,84
1,88
1,92
1,96
2,00
2,04
2,08
2,12
2,16
2,20
2,24
2,27

Clases	Marcas de clase (x_i)	Recuento	n_i	n_i acumuladas	h_i	h_i acumuladas
1,775-1,825	1,80	/	1	1	0,01	0,01
1,825-1,875	1,85	///	5	6	0,05	0,06
1,875-1,925	1,90	/// /// /	11	17	0,11	0,17
1,925-1,975	1,95	/// /// /// ///	20	37	0,20	0,37
1,975-2,025	2,00	/// /// /// ///	33	70	0,33	0,70
2,025-2,075	2,05	/// /// /// //	17	87	0,17	0,87
2,075-2,125	2,10	/// ///	10	97	0,10	0,97
2,125-2,175	2,15		0	97	0,00	0,97
2,175-2,225	2,20	//	2	99	0,02	0,99
2,225-2,275	2,25	/	1	100	0,01	1,00

Para representar una distribución de frecuencias agrupadas, son tres los procedimientos:

— histograma de frecuencias,
— polígono de frecuencias,
— polígono acumulativo.

El *histograma de frecuencias* se construye dibujando sobre cada intervalo de clase rectángulos de áreas proporcionales a las frecuencias respectivas.

Si los intervalos de clase son iguales, las bases de los rectángulos del histograma también lo son y, entonces, sus alturas son proporcionales (iguales) a las frecuencias.

El *polígono acumulativo* se construye de la siguiente manera: dispuestas las clases como en el histograma de frecuencias, sobre el eje horizontal, partiendo del extremo inferior del primer intervalo, con ordenada 0, se une con el otro extremo a una altura que sea numéricamente igual al área del primer rectángulo (si los intervalos son iguales, coincide con la altura del rectángulo). Se une ese punto con otro del extremo superior de la segunda clase, cuya ordenada sea numéricamente igual a la suma de las áreas de los dos primeros rectángulos (suma de sus alturas, si se trata de intervalos de igual longitud), y así sucesivamente.

El polígono acumulativo es muy útil. Si se traza por la abscisa x_i la ordenada que corta al polígono en P, y por P se traza la paralela al eje de abscisas, ésta intercepta en el eje de ordenadas un punto A que da la frecuencia n_i o/y h_i de individuos cuyo valor de la variable es menor o igual que x_i.

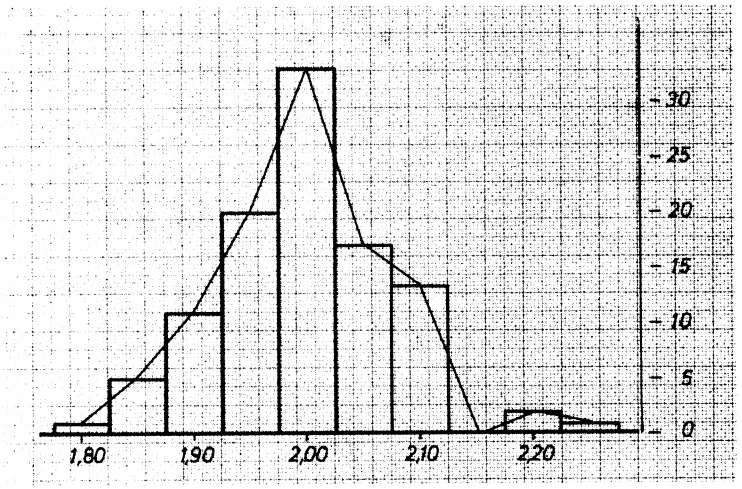
El *polígono de frecuencias* es la poligonal cuyos vértices son los puntos medios de las bases superiores de los rectángulos del histograma de frecuencias.

Las gráficas de la página siguiente corresponden al ejemplo que se viene desarrollando.

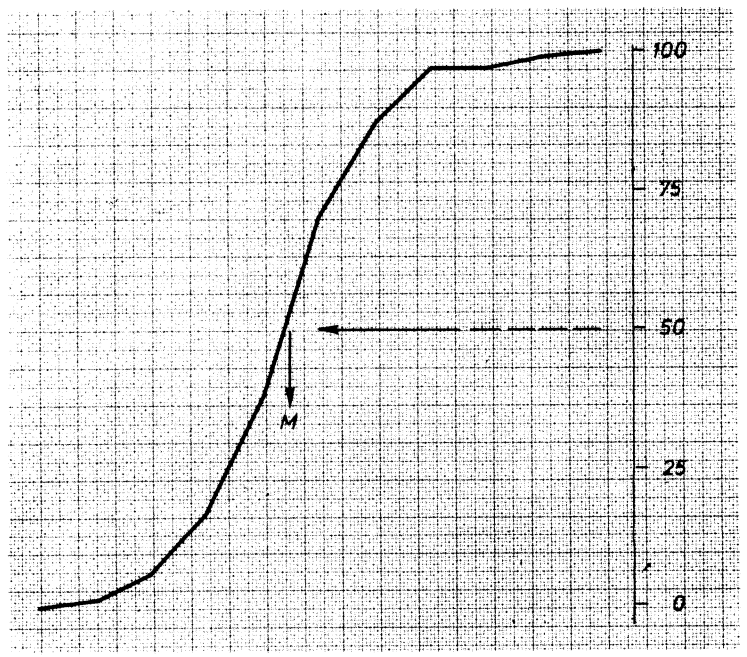
3.524. Reducción de la información: estadísticos

Una vez recogidos, tabulados y representados los datos de la serie estadística, es necesario reducir toda esa información a unos números representativos de la distribución, que reciben el nombre de *características estadísticas* o *estadísticos*.

Ellos permiten, de una forma cuantitativa, al margen de todo subjetivismo,



Histograma y polígono de frecuencias



Polígono acumulativo

la comparación entre distintas series estadísticas y la valoración en números, de sus diversas características.

Son de cuatro clases estas medidas: los estadísticos de *centralización* suministran los valores centrales o promedios, alrededor de los cuales se agrupan los datos de la serie; los de *dispersión* miden la mayor o menor regularidad de agrupamiento de la serie, sobre las medidas centrales; las medidas de *asimetría* cuanti-

fican, como su nombre indica, la asimetría de la distribución; por último se citan los estadísticos de *prominencia* que son capaces de comparar, a igualdad de dispersión, la densidad de frecuencias extremas y centrales.

En una visión de conjunto, como índice previo de los diferentes términos que se van a desarrollar a continuación, se suministra el siguiente cuadro:

- Estadísticos
  - Centralización o posición.....
    - medias
      - aritmética { simple, ponderada }
      - geométrica
      - cuadrática
      - armónica
    - mediana
    - moda
  - Dispersión o variabilidad..
    - Recorrido o intervalo total
    - Intervalos centrales
    - Cuantiles o percentiles
      - — cuartiles
      - — deciles
      - — recorrido intercuartílico
      - — mediana respecto de la $\bar{x}$
    - Desviación media respecto de la M
    - Varianza y desviación típica
    - Coeficiente de variación o dispersión
    - Tipificación de la variable.
  - Asimetría.....
    - Coeficiente de asimetría
    - Coeficiente de Pearson
  - Prominencia ...
    - Coeficiente de prominencia

3.5241. *Estadísticos de centralización*

Medias. De las cuatro medias posibles: aritmética, geométrica, cuadrática y armónica, describiremos las dos primeras:

Media aritmética

Sea la variable X que toma los valores $x_1, x_2, \ldots x_k$, con las frecuencias absolutas $n_1, n_2, \ldots n_k$, de modo que el cardinal de la muestra es $n_1 + n_2 + \cdots + n_k = N$.

Se denomina media aritmética de la distribución al estadístico que define la siguiente fórmula:

$$\bar{x} = \frac{x_1 \cdot n_1 + x_2 \cdot n_2 + \cdots + x_k \cdot x_k}{N} = \frac{1}{N} \sum_{i=1}^{k} x_i \cdot n_i \qquad [1]$$

Si en la expresión [1] se dispone la fracción completa en suma de fracciones simples de denominador común N resulta:

$$\bar{x} = x_1 \cdot \frac{n_1}{N} + x_2 \cdot \frac{n_2}{N} + \ldots + x_k \cdot \frac{n_k}{N} = x_1 h_1 + x_2 h_2 + \ldots x_k h_k$$

$$\bar{x} = \sum_{i=1}^{k} x_i h_i \qquad [1']$$

expresión de la media, en función de las frecuencias relativas.

Ejemplo

A partir de ahora, y si nada se dice en contrario, todos los cálculos se referirán al ejemplo que hemos venido desarrollando de los espesores de las 100 piezas fabricadas en serie por una factoría eléctrica.

La media de su distribución de frecuencias agrupadas es

$$\bar{x} = \frac{1}{100}(1{,}80 \times 1 + 1{,}85 \times 5 + 1{,}90 \times 11 + \ldots + 2{,}25 \times 1) = 1{,}9945 \text{ mm}$$

Más adelante, cuando se haya establecido el concepto de desviación típica, se mostrará la forma práctica de establecer los cálculos de ambos estadísticos, disponiendo tablas operativas adecuadas.

A los elementos de un conjunto de valores $X = \{x_1, x_2, \ldots x_n\}$ se les asocian los elementos p_i del «conjunto de ponderación $N \supset P = \{p_1, p_2, \ldots p_n\}$ y se define —de un modo general— *media aritmética ponderada* de la serie X por la fórmula

$$\bar{x} = \frac{x_1p_1 + x_2p_2 + \cdots + x_np_n}{p_1 + p_2 + \cdots + p_n}$$

$$\bar{x} = \frac{\sum_{i=1}^{n} x_ip_i}{\sum_{i=1}^{n} P_i} \qquad [2]$$

Los elementos de P pueden llamarse «pesos o valoraciones» e indican la importancia relativa de cada uno de los elementos de X.

Adviértase que, por tratarse de frecuencias agrupadas, la media aritmética escrita en [1] no es más que una media aritmética ponderada.

Media geométrica

Sobre la distribución de frecuencias de la variable X, de N datos, se establece la media geométrica de la serie, mediante la fórmula

$$\bar{x}_g = \sqrt[N]{x_1 \cdot x_2 \cdot \ldots \cdot x_n} \qquad [3]$$

o bien

$$\bar{x}_g = \left(\prod_{i=1}^{n} x_i\right)^{1/N} \qquad [3']$$

Presenta dos inconvenientes que la hacen de poco uso: uno, que si un dato es nulo, resulta 0; otro, que su cálculo suele ser laborioso.

Moda

Moda de una distribución de frecuencias es la marca de la clase (o el valor de la variable, si no están agrupadas las frecuencias) de mayor frecuencia. O sea, el valor de la variable que la ostenta mayor número de individuos de la muestra.

Se comprende que puede existir más de una moda, en cuyo caso se trata de una *distribución multimodal.*

La moda de la distribución de nuestro ejemplo es

$$x_5 = 2{,}00 \text{ mm}$$

con sus $n_5 = 33$ individuos, que la ostentan.

Mediana

Este estadístico de centralización, que también se puede considerar de dispersión o variabilidad, se define como el valor de la variable, M, tal que el 50 por 100 de los individuos de la distribución alcanzan un valor superior a M y el otro 50 por 100 toman un valor de la variable igual o menor que M.

A) La determinación de la mediana en series discretas o continuas no agrupadas se puede hacer analítica o gráficamente:

A_1) Analíticamente:

Basta ordenar la serie de menor a mayor valor de x_i y detectar el término central, que será la mediana (si existieran dos términos centrales, la mediana es la media aritmética de ellos.)

Dispuestas las cien medidas del ejemplo, de menor a mayor, la que ocupa el lugar quincuagésimo es 1,99 mm; luego la mediana de esa serie continua de frecuencias no agrupadas es

$$M = 1{,}99 \text{ mm}$$

A_2) Gráficamente:

Es suficiente para determinar la mediana de este modo trazar sobre el diagrama acumulativo la recta $y = 0{,}5$, que cortará en un punto al diagrama, cuya abscisa es el valor de la mediana.

En el diagrama acumulativo de la página 395 se determina así la mediana.

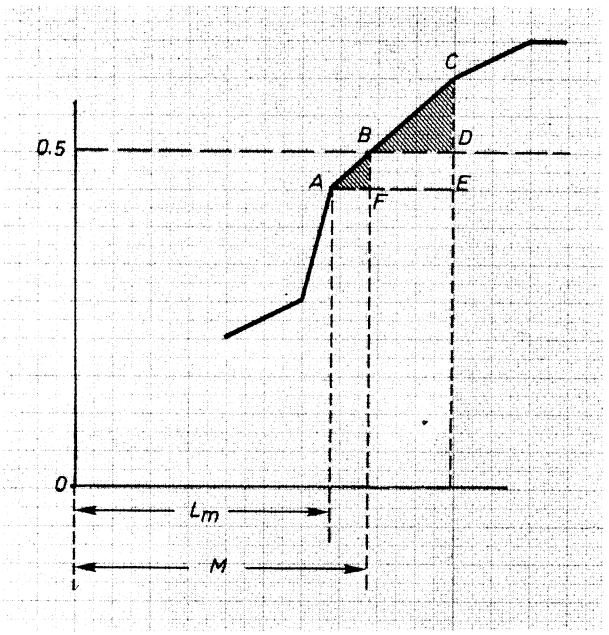
B) Si se trata de series de frecuencias agrupadas, el método gráfico-analítico para su determinación produce la siguiente fórmula para el valor de la mediana:

$$M = L_m + \frac{N/2 - \Sigma n}{n_m} \cdot i \qquad [4]$$

en la que

L_m = límite inferior de la clase-mediana
$N/2$ = mitad del número de observaciones
Σn = número de datos por debajo de la clase-mediana
n_m = datos de la clase-mediana
i = longitud del intervalo

La deducción de la fórmula [4] es la sencilla aplicación de una semejanza de triángulos que se producen al cortar con $y = 0{,}5$ al polígono acumulativo de la distribución.



$$M = L_m + \overline{HI} = L_m + \overline{AF};$$

$$\overline{AF} = \frac{N/2 - \Sigma n}{n_m} \cdot \overline{AE}$$

Para determinar la mediana de nuestro ejemplo, lo primero de todo hay que detectar cuál es la clase-mediana. Para ello basta consultar la columna de frecuencias acumuladas de la tabla de su distribución y observar que la clase $x_4 = 1{,}95$ acumula treinta y siete observaciones hasta ella y que la clase $x_5 = 2{,}00$ alcanza 70 observaciones inferiores o iguales a ella.

Como $N = 100$ y $70 > N/2$, es claro que la mediana ha de buscarse en ese quinto intervalo.

$$\left.\begin{array}{l} L_m = 1{,}975 \\ \Sigma_n = 37 \\ n_m = 33 \\ i = 0{,}05 \end{array}\right\} \quad M = 1{,}975 + \frac{50 - 37}{33} \cdot 0{,}05 = 1{,}995 \text{ mm}$$

Sobre el polígono acumulativo de la página 397 se ha marcado la localización de la mediana.

3.5242. *Estadísticos de dispersión*

Recorrido o intervalo total

El intervalo total de una distribución de frecuencias es la diferencia entre los valores extremos que toma la variable.

Es un estadístico de consideración inevitable, pero de muy pobre información:

un solo valor extremadamente desviado (por pequeño o por grande) de la distribución «alargaría» el intervalo total en una longitud que podría inducir a error, al inferir conclusiones.

El intervalo total de la distribución que venimos analizando es

$$\Delta x = 2{,}27 - 1{,}80 = 0{,}47 \text{ mm}$$

Fractiles, cuantiles o percentiles; cuartiles; recorrido intercuartílico

Se llama fractil, cuantil o percentil del m por 100 en una distribución de frecuencias a un valor de la variable, x_m, tal que el m por 100 de los individuos de la muestra ostenta un valor menor o igual a x_m, mientras que el $(100 - m)$ por 100 restante alcanza un valor superior a x_m.

La determinación es idéntica a la de la mediana; al fin y al cabo, la mediana no es más que el fractil del 50 por 100.

$$x_m = L_m + \frac{\frac{N \cdot m}{100} - \Sigma n}{n_m} \cdot i \qquad [5]$$

Todos los términos que aparecen en la fórmula [5] simbolizan los conceptos correspondientes a los que simbolizaban en la de la mediana, [4].

La determinación gráfica sobre el polígono acumulativo, análogamente, se consigue trazando la recta $y = m/100$, que cortará al polígono en el punto cuya abscisa es el fractil x_m.

Determinemos, por ejemplo, el fractil del 20 por 100 de la distribución de espesores.

Primero habrá que encontrar la clase a la que pertenece el percentil buscado: es la cuarta, de marca $x_4 = 1{,}95$, pues, como $N = 100$, el 20 por 100 de los individuos es veinte; la tercera acumulada hasta diecisiete y la cuarta llega a treinta y siete observaciones.

$$\left.\begin{aligned} L_{20\%} &= 1{,}925 \\ \Sigma n &= 17 \\ n_{20\%} &= 20 \\ i &= 0{,}05 \end{aligned}\right\} \quad x_{20\%} = 1{,}925 + \frac{20 - 17}{20} \cdot 0{,}05 = 1{,}9325 \text{ mm.}$$

El 20 por 100 de las piezas tiene un espesor menor o igual a 1,9325 mm.

Los fractiles más usados son los del 25 y del 75 por 100, denominados *primer cuartil* y *tercer cuartil*, respectivamente. La mediana resulta ser, así, el segundo cuartil.

El *recorrido intercuartílico* es un estadístico de dispersión que se calcula mediante la diferencia entre el tercer y primer cuartiles, y es el intervalo central del 50 por 100, que reúne entre sus valores extremos al 50 por 100 de los individuos de la muestra, localizados en la mitad central de la distribución.

Recorrido intercuartílico de la muestra de espesores de piezas

$$\left.\begin{array}{r} L_{25\%} = 1{,}925 \\ \Sigma n = 17 \\ n_{25\%} = 20 \\ i = 0{,}05 \end{array}\right\} \quad x_{25\%} = 1{,}925 + \frac{25 - 17}{20} \cdot 0{,}05 = 1{,}945 \text{ mm.}$$

$$\left.\begin{array}{r} L_{75\%} = 2{,}025 \\ \Sigma n = 70 \\ n_{75\%} = 17 \\ i = 0{,}05 \end{array}\right\} \quad x_{75\%} = 2{,}025 + \frac{75 - 70}{17} \cdot 0{,}05 = 2{,}040 \text{ mm.}$$

$$\delta_x = x_{75\%} - x_{25\%} = 0{,}095 \text{ mm.}$$

El 50 por 100 de las piezas de espesores intermedios presentan diferencias inferiores a una décima de milímetro.

La determinación gráfica, tanto de los cuartiles como del recorrido intercuartílico, es idéntica a como se hace con cualquier fractil, sobre el polígono acumulativo.

La fijación de los fractiles sobre el histograma de frecuencias determina sobre éste áreas de igual valor al fractil; de modo que, por ejemplo, levantadas las ordenadas de los cuartiles primero y tercero, queda determinada una superficie central igual a 0,5, puesto que el área total del histograma ha de ser la unidad. Dibujada la ordenada del fractil x_{20}, ésta deja a su izquierda una superficie de área 0,2 y a su derecha, otra de área 0,8.

Desviación media

Respecto de la media: Este estadístico refleja la dispersión de los valores que toma la variable, respecto de la media. Cuanto más y mayores sean las diferencias de las observaciones a la media, más elevada es la desviación media. Se calcula mediante la fórmula

$$D_m = \frac{1}{N} \sum_{i=1}^{k} n_i |x_i - \bar{x}| \qquad [6]$$

o bien

$$D_m = \sum_{i=1}^{k} h_i |x_i - \bar{x}| \qquad [6']$$

Respecto de la mediana: La desviación media respecto de la mediana indica análoga variabilidad de dispersión que la anterior, pero aquí, referible a la mediana. Su fórmula es

$$D_M = \sum_{i=1}^{k} h_i |x_i - M| \qquad [7]$$

Varianza; *desviación típica*; *momentos*

La desviación típica, σ, y su cuadrado, σ^2, la varianza, son —con mucho— los estadísticos más útiles para medir la dispersión de una distribución.

Las fórmulas que siguen establecen los dos conceptos.

Varianza

$$\sigma^2 = \frac{\sum_{i=1}^{k} (x_i - \bar{x})^2 n_i}{N} \qquad [8]$$

o bien

$$\sigma^2 = \sum_{i=1}^{k} h_i (x_i - \bar{x})^2 \qquad [8']$$

Desviación típica

$$\sigma = \sqrt{\frac{\sum_{i=1}^{k} (x_i - \bar{x})^2 n_i}{N}} \qquad [9]$$

o en frecuencias relativas

$$\sigma = \sqrt{\sum_{i=1}^{k} h_i (x_i - \bar{x})^2} \qquad [9']$$

En Estadística descriptiva son muy frecuentes expresiones como ésta:

$$\sum_{i=1}^{k} h_i x_i^n.$$

La frecuencia de su aparición justifica que se les haya dado nombre específico: se denominan *momentos*, de modo que una expresión como la apuntada es el momento de orden n (por ser n el exponente de la x_i)

$$a_n = \sum_{i=1}^{k} h_i x_i^n \qquad [10]$$

Para el cálculo de la varianza y desviación típica se puede hacer una pequeña deducción, a partir de la fórmula [9'] y conseguir otra fórmula que evite el engorroso cálculo de las diferencias cuadráticas. En efecto: a continuación se calcula la desviación típica en función del momento de segundo orden.

$$\sigma = \sqrt{\sum_{i=1}^{k} h_i (x_i - \bar{x})^2} = \sqrt{\sum_{i=1}^{k} h_i (x_i^2 + \bar{x}^2 - 2\bar{x}x_i)} =$$

$$= \sqrt{\sum_{i=1}^{k} h_i x_i^2 + \bar{x}^2 \sum_{i=1}^{k} h_i - 2\bar{x} \sum_{i=1}^{k} h_i x_i}$$

Pero el segundo término del radicando vale $\bar{x}^2$, ya que $\sum_{i=1}^{k} h_i = 1$, y el tercer término resulta ser $-2\bar{x}^2$, puesto que

$$\sum_{i=1}^{k} h_i x_i = \bar{x}.$$

Reduciendo,

$$\sigma = \sqrt{\sum_{i=1}^{k} h_i x_i^2 - \bar{x}^2} \qquad [11]$$

Adviértase que el primer término del radicando de [11] es el momento de segundo orden, resultando, en definitiva

$$\sigma = \sqrt{a_2 - \bar{x}^2} \qquad [11']$$

fórmula de la desviación típica, en función del momento de segundo orden.

Como se prometió en la página 399, a continuación se disponen las tablas operativas y cálculos de la media y de la desviación típica de la distribución que nos viene sirviendo para concretar.

La tabla, junto a algunas de las columnas descriptivas con que aparecía en la página 396 se aumenta con otras nuevas de carácter operativo, cuyas cabeceras indican los cálculos a que se refieren.

Entiéndase que, por ser más cómodo operar enteros que decimales, para calcular, por ejemplo, $\sum_{i=1}^{k} h_i x_i^2$, lo que se hace es calcular $\sum_{i=1}^{k} n_i x_i^2$, dividiendo después por N.

x_i	n_i	$n_i x_i$	x_i^2	$n_i x_i^2$
1,80	1	1,80	3,24	3,24
1,85	5	9,25	3,43	17,15
1,90	11	20,90	3,61	39,71
1,95	20	39,—	3,80	76,—
2,00	33	66,—	4,—	132,—
2,05	17	34,85	4,20	71,40
2,10	10	21,—	4,41	44,10
2,15	0	0	0	0
2,20	2	4,40	4,84	9,68
2,25	1	2,25	5,06	5,08
		$\Sigma n_i x_i = 199{,}45$		$\Sigma n_i x_i^2 = 398{,}34$

$$\bar{x} = \frac{\sum_{i=1}^{k} n_i x_i}{N} = 1{,}9995 \text{ mm}$$

$$\sigma = \sqrt{\sum_{i=1}^{k} h_i x_i^2 - \bar{x}^2} =$$

$$= \sqrt{3{,}9834 - 3{,}9780}$$

$$\sigma = 0{,}074 \text{ mm}$$

Método abreviado para el cálculo de la media y la desviación típica

Todavía se puede intentar abreviar los cálculos, lo que se consigue haciendo el cambio de variable que indica la siguiente igualdad

$$x_i = i \cdot u_i + x_0 \qquad [12]$$

en la que

x_i = variable tabulada
i = intervalo de clase
u_i = nueva variable
x_0 = origen de trabajo

Tomando como origen de trabajo un valor promedio de los valores de x_i, con este cambio se consiguen manipular números enteros, en lugar de los engorrosos decimales.

Se obtiene así la media en términos de la nueva variable, $\bar{u}$, pero el paso a $\bar{x}$ no puede ser más sencillo, como se justifica a continuación.

La desviación típica se obtiene directamente.

A) *Cálculo abreviado de la media*

$$\bar{x} = \sum_{i=1}^{k} x_i h_i = x_1 h_1 + x_2 h_2 + \ldots + x_k h_k \qquad [13]$$

Sustituyendo en [13] el cambio [12], resulta:

$$\bar{x} = h_1(i \cdot u_i + x_0) + h_2(i \cdot u_2 + x_0) + \ldots + h_k(i \cdot u_k + x_0)$$

$$\bar{x} = i \cdot (h_1 u_1 + h_2 u_2 + \ldots + h_k u_k) + x_0 \cdot (h_1 + h_2 + \ldots + h_k)$$

$$\bar{x} = i \cdot \bar{u} + x_0 \qquad [14]$$

Bastará, pues, calcular $\bar{u}$, para luego, sencillamente, obtener $\bar{x}$

$$\bar{u} = \frac{1}{N} \sum_{i=1}^{k} u_i n_i \qquad [15]$$

B) *Cálculo abreviado de la desviación típica*

$$\begin{array}{ll} \text{I} & x_i = i \cdot u_i + x_0 \\ \text{II} & \bar{x} = i \cdot \bar{u} + x_0 \end{array}$$

$$x_i - \bar{x} = i \cdot (u_i - \bar{u}) \qquad [16]$$

Según la [9']

$$\sigma = \sqrt{\sum_{i=1}^{k} h_i (x_i - \bar{x})^2} \, .$$

Sustituyendo [16]

$$\sigma = \sqrt{\sum_{i=1}^{k} h_i \cdot i^2 \cdot (u_i - \bar{u})^2}$$

Siendo i constante, sale fuera del signo radical, y operando,

$$\sigma = i \cdot \sqrt{\sum_{i=1}^{k} h_i (u_i^2 + \bar{u}^2 - 2\bar{u}u_i)}$$

$$\sigma = i \cdot \sqrt{\sum_{i=1}^{k} h_i u_i^2 + \bar{u}^2 \sum_{i=1}^{k} h_i - 2\bar{u} \sum_{i=1}^{k} h_i u_i} \qquad [17]$$

Como

$$\sum_{i=1}^{k} h_i = 1 \quad \text{y} \quad \sum_{i=1}^{k} h_i u_i = \bar{u},$$

sustituyendo en [17],

$$\sigma = i \cdot \sqrt{\sum_{i=1}^{k} h_i u_i^2 - \bar{u}^2} \qquad [18]$$

Como se observará, la [18] es en todo análoga a la [11], pero descrita en la nueva variable u.

A continuación, se concretan estos cálculos abreviados de la media y de la desviación típica sobre nuestro ejemplo-base.

Cambio de variable:

$$x_i = i \cdot u_i + x_0 \Rightarrow u_i = \frac{1}{i}(x_i - x_0)$$

$i = 0{,}05$

$x_0 = 2{,}00$ (uno de los valores centrales de x_1, tomado arbitrariamente)

Cálculo de u_1:

$$u_1 = \frac{1}{0{,}05} \cdot (1{,}80 - 2) = -4$$

Los restantes se tabulan

u_i	n_i	$u_i n_i$	u_i^2	$n_i u_i^2$
−4	1	4	16	16
−3	5	−15	9	45
−2	11	−22	4	44
−1	20	−20	1	20
0	33	0	0	0
1	17	17	1	17
2	10	20	4	40
3	0	0	9	0
4	2	8	16	32
5	1	5	25	25
	$\Sigma n_i = 100$	$\Sigma u_i n_i = -11$		$\Sigma n_i u_i^2 = 239$

$$\bar{u} = \frac{-11}{100} = -0{,}11 \Rightarrow \bar{x} = 0{,}05 \cdot (-0{,}11) + 2 = 1{,}9945 \text{ mm}$$

$$\sigma = 0{,}05 \cdot \sqrt{2{,}39 - 0{,}0121} = 0{,}05 \times 1{,}50 = 0{,}075 \text{ mm}$$

Coeficiente de variación o dispersión

Conviene fijar la variabilidad relativa de una muestra, pues es muy diferente decir que la desviación media, por ejemplo, es 4 unidades en una muestra de media 80, que en otra, de media 8.

Para medir esta variabilidad relativa se usa el llamado coeficiente de variación o dispersión, que es el cociente entre la desviación típica y la media:

$$d = \frac{\sigma}{\bar{x}} = \frac{\sqrt{\sum_{i=1}^{k} h_i(x - \bar{x})^2}}{\sum_{i=1}^{k} h_i x_i} \qquad [19]$$

Sobre la [19] se pueden hacer todos los cálculos abreviados y sustituciones que se vienen realizando en los otros estadísticos.

Adviértase que este coeficiente d es adimensional, lo que le hace idóneo para comparar series descritas en distintas unidades.

En esta línea de comparación de individuos de la misma o distintas muestras, el método más conveniente de realizarla es la

Tipificación de la variable

Se trata del cambio de variable que se expresa

$$z_i = \frac{x_i - \bar{x}}{\sigma} \qquad [20]$$

Los valores tipificados vienen medidos por el número de desviaciones típicas de la diferencia de cada valor a la media

Ejercicio. Justifíquese que una muestra descrita en valores tipificados, tiene de media 0 y de desviación típica 1.

3.5243. *Estadísticos de asimetría. Momentos centrales*

A) Coeficiente de asimetría

En Estadística descriptiva suelen aparecer con suficiente frecuencia expresiones como ésta:

$$\sum_{i=1}^{k} h_i(x_i - \bar{x})^n \qquad [21]$$

Se denotan m_n y se llaman momentos centrales de orden n.

Con ello, digamos que para medir la mayor o menor asimetría de una distribución se usa el llamado *coeficiente de asimetría*, k, que es el cociente entre el momento central de orden 3 y el cubo de la desviación típica.

$$k = \frac{m_3}{\sigma^3} = \frac{1}{\sigma^3} \sum_{i=1}^{k} h_i(x_i - \bar{x})^3 \qquad [22]$$

Efectivamente, k es un número adecuado para medir lo que pretende, ya que se anula cuando la distribución es perfectamente simétrica y $|k|$ es tanto mayor cuanto más asimétrica sea. Más aún, el signo de k indica el sentido de la asimetría.

B) Coeficiente de Pearson

La asimetría puede también medirse mediante este estadístico, cuya expresión es

$$k_p = \frac{\bar{x} - \text{moda}}{\sigma} \qquad [23]$$

Cuanto más asimétrica sea una distribución, más separadas se encuentran su media y su moda, más grande será el coeficiente de Pearson. Además, el signo de éste indica el sentido de la asimetría.

3.53. ESTADISTICA DESCRIPTIVA ; DISTRIBUCIONES BIVARIANTES

3.531. Dependencia funcional y aleatoria: variables estadísticas bidimensionales

Sea una masa de gas ideal que va tomando distintos estados, en condiciones isotermas, es decir, manteniendo constante su temperatura: $dT = 0$.

A medida que se varía la presión (p), el volumen (V) de esa masa de gas adquiere diferentes valores, obedeciendo la conocida ley de Boyle-Mariotte, que exige que

$$p \cdot V = k \text{ (constante)} \qquad [24]$$

Existe una rigurosa *dependencia funcional* o analítica entre las dos variables de estado, p y V: fijada una presión p_1, la masa de gas, experimentada isotérmicamente, ocupa «necesariamente» un determinado volumen V_1; si es p_2 la presión, entonces su volumen será un número fijo, V_2, de modo que

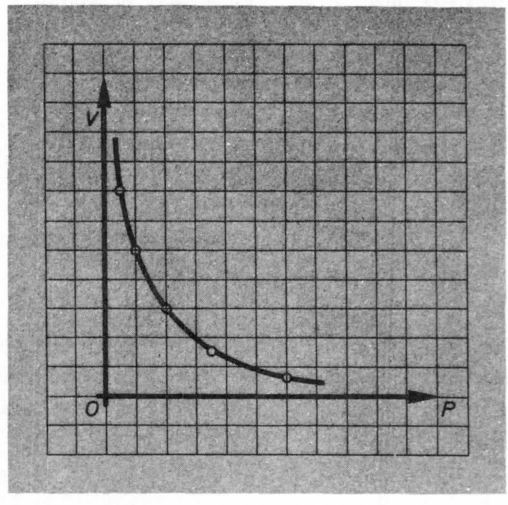
$$p_1 \cdot V_1 = p_2 \cdot V_2 = k \text{ (constante)};$$

y, en general,

$$p_i \cdot V_i = k$$

Si se disponen unos ejes cartesianos para representar el fenómeno, registrando presiones en abscisas y volúmenes en ordenadas, cada estado isotermo de la masa de gas experimentada vendrá representado por un punto del plano: por el punto (p_i, V_i). Se consigue así, una bien conocida línea: una rama de hipérbola equilátera, que es la representación gráfica de la función analítica $p \cdot V = k$, en la que sus variables presentan *dependencia funcional.*

p	V
p_1	V_1
p_2	V_2
.	.
.	.
.	.
p_i	V_i



Existen multitud de fenómenos en la Naturaleza, de todo tipo, que no admiten el tratamiento matemático anterior, pero que vienen fijados por dos variables, de alguna manera dependientes entre sí. Tal sería el caso, por ejemplo, de las alturas alcanzadas por plantas de maíz, en función del tiempo de su germinación. Ciertamente, cuantas más semanas hayan transcurrido desde su nacimiento, más altura alcanzará el tallo; pero lo que no sucede es que, dado un determinado tiempo, t_i, a partir del momento de su germinación, exista una altura perfectamente fija y determinada que le corresponda, a_i.

Claro es que el tiempo y la altura dependerán de alguna manera entre sí, pero con una dependencia mucho menos «robusta» que la funcional; se dice que presentan una *dependencia aleatoria*.

Por analogía con el lenguaje analítico, establecemos la función aleatoria

$$f(t, a) = 0$$

y diremos que se trata de una *variable estadística bidimensional*.

En las distribuciones estadísticas de variables bidimensionales, cada individuo de la muestra viene caracterizado por un par de números, que son los valores que toman las dos variables, en cada caso.

El modo más simple de representación de una distribución estadística bidimensional viene sugerido por la representación cartesiana de las funciones analíticas. Como allí, se disponen unos ejes de coordenadas ortogonales y sobre el eje de abscisas se representan los valores de una de las variables, y sobre el de ordenadas, los de la otra. De este modo, cada individuo de la muestra queda representado por un punto del plano cartesiano.

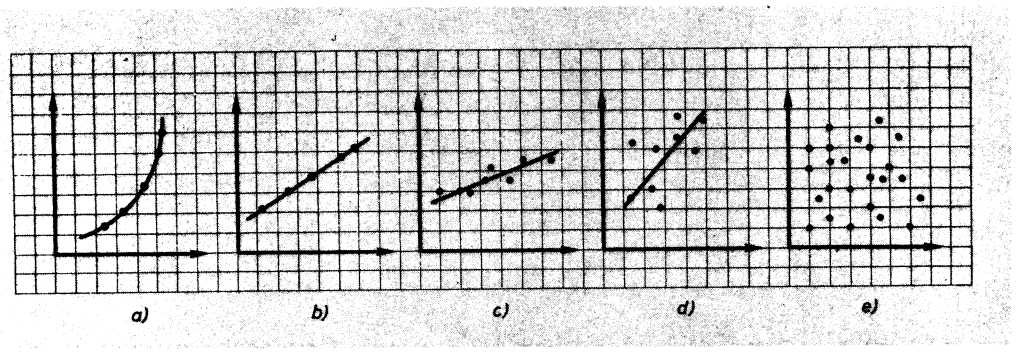
Esta manera de representación recibe el nombre de *nube de puntos* o *diagrama de dispersión*.

De un modo intuitivo, y en espera de mayor precisión, cabe observar ahora que, si la nube de puntos se constriñe mucho y éstos aparecen agrupados alrededor de una posible línea representativa, es señal de que la dependencia aleatoria entre las dos variables estadísticas es bastante fuerte; mientras que si el diagrama de

puntos resulta ser muy disperso, y de ninguna manera sugiere una posible línea representativa del fenómeno, ello es debido a que la dependencia entre las dos variables estadísticas representadas es muy débil. Como casos extremos, entiéndase que si la nube de puntos cubre todo el plano, en dispersión total, la presunta dependencia aleatoria no existe; y que, si por el contrario, al representar una distribución estadística bivariante se obtiene un diagrama de puntos, formado por todos los que están sobre una determinada línea, la dependencia deja de ser aleatoria para ser funcional.

Los ejemplos que siguen esquematizan los conceptos precedentes.

Ejemplos



Sobre muestras imaginarias bidimensionales,

dependencia funcional { parabólica *a*) / lineal *b*)

dependencia aleatoria { fuerte *c*) / débil *d*)

independencia aleatoria *e*)

3.532. Tablas y gráficos

Ya queda apuntada la forma más simple de representación de una distribución aleatoria bivariante: el diagrama de puntos.

La tabulación de datos de una variable estadística bidimensional se realiza mediante una tabla de doble entrada. En cada una de las cuadrículas de estas tablas se registran las frecuencias absolutas de cada una de las clases bidimensionales. Así, si en una de ellas aparece el número n_{ij}, se quiere indicar que existen n_{ij} individuos cuyo carácter bidimensional es (i, j); es decir, que hay ese número de individuos con un valor i de la variable X y con un valor j de la variable Y.

Ejemplo.

Volvamos sobre nuestro ejemplo-base que nos ha venido sirviendo para describir distribuciones monovariantes: se trataba de 100 piezas de serie, estudiadas en función de sus espesores. Se había hecho una distribución de frecuencias agrupadas en diez clases de espesores.

Ahora establecemos la variable bidimensional sobre esa misma muestra

(espesor, conductividad).

Medida la conductividad de las 100 piezas, se ha realizado su estudio monovariante y se han creado 5 clases con las siguientes marcas

$$y_i\colon \quad 1.800 \ ; \ 1.900 \ ; \ 2.000 \ ; \ 2.100 \ ; \ 2.200 \ \mu\Omega^{-1}$$

Como se hiciera con los espesores (x_i), a fin de realizar un cálculo abreviado de los estadísticos, se transformaron las y_i en w_i, y se obtuvieron estas marcas, elaboradas según el cálculo $w_i = \dfrac{1}{100} \cdot (y_i - y_0)$;

$$w_i\colon \quad -2 \ ; \ -1 \ ; \ 0 \ ; \ 1 \ ; \ 2 \qquad\qquad y_0 = 2.000$$

Hecho el recuento, las frecuencias han resultado ser las que se indican en la tabla.

Distribución bivariante de frecuencias de la muestra de cien piezas eléctricas, respecto de la variable (espesor, conductividad) en (mm, $\mu\Omega^{-1}$). Variables codificadas a u_i y w_i.

(x, y)		Espesor (x) mm										
Conductividad (y) $\mu\Omega^{-1}$	u_i / ω_i	-4	-3	-2	-1	0	1	2	3	4	5	Σn ↓
	-2	1	2	2								5
	-1		3	8	9							20
	0			1	10	32	10	5		2		60
	1				1	1	6	2				10
	2						1	3			1	5
	Σn →	1	5	11	20	33	17	10	0	2	1	100

Las representaciones gráficas de estas distribuciones estadísticas bivariantes, aparte del ya citado *diagrama de dispersión*, son los *diagramas de ordenadas* y los *prismogramas*. Los primeros son adecuados cuando los dos caracteres de la variable

son cualitativos o cuantitativos discretos; un prismograma es la representación adecuada si ambos caracteres de la variable presentan una distribución cuantitativa continua.

Para construir un diagrama de ordenadas, se disponen unos ejes cartesianos tridimensionales, y en los ejes x e y del plano-base se representan los diversos valores o rúbricas de las dos variables. De este modo se consigue una cuadrícula-base en la que cada uno de sus nudos representa una clase bivariante (x_i, y_i). Basta levantar segmentos perpendiculares en cada uno de los puntos, de longitud proporcional a las respectivas frecuencias, para completar el diagrama.

Para realizar un prismograma, se dispone, como antes, un triedro trirrectángulo. Representados en cada uno de los ejes del plano-base los intervalos en que se distribuyen cada uno de los caracteres continuos, x e y, se levantan, con base en las cuadrículas que resultan, prismas cuya altura (y cuyo volumen, si los intervalos son iguales) son proporcionales a las frecuencias de caea clase bivariante, (x_i, y_i).

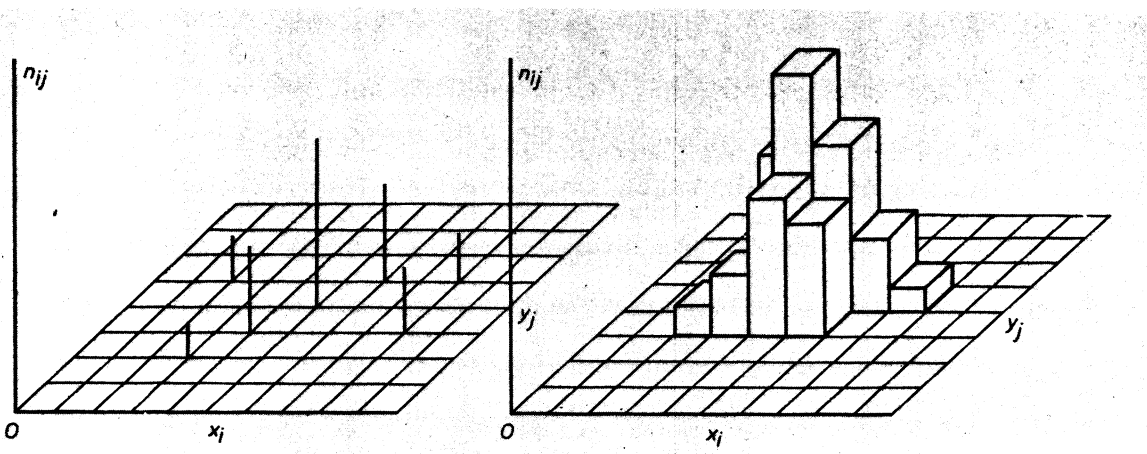


Diagrama de ordenadas y prismograma de dos distribuciones aleatorias bivariantes, imaginarias.

3.533. Regresión. Regresión lineal

La mayor o menor dependencia aleatoria entre los caracteres de una variable estadística bivariante se pone de manifiesto porque al realizar su diagrama de puntos aparecen éstos más o menos localizados en una determinada zona, que puede recordar una línea matemática de algún tipo: recta, parábola, hipérbola, etc. Pues bien, cuando en una muestra bivariante sucede que «aproximadamente» uno de los caracteres se puede considerar función del otro y, consecuentemente, la distribución puede quedar razonablemente representada por una determinada función matemática, se dice que existe *regresión* de los valores de uno de los caracteres respecto de los de otro.

A la línea que representa la distribución se le llama *línea de regresión* y, claro

es, que se podrá hablar de regresión lineal, hiperbólica, parabólica, etc., según sea la línea que represente la distribución.

No existe razón lingüística para tal nombre. El motivo es, simplemente, histórico. En 1886, Galton publicaba un trabajo estadístico sobre la talla de los padres y la de la generación filial. Observó que, ciertamente, a padres altos correspondían hijos, también, de elevada estatura y que padres de poca talla tenían, en general, hijos bajos. Pero, a la vez, se dio cuenta de que la estatura de los hijos, aun con las rúbricas apuntadas, tendían a «regresar» a la media de la raza; o sea, que padres altos engendraban hijos altos, pero menos que ellos; y que padres de poca talla tenían hijos bajos, pero más altos que ellos. Todo indicaba como si la estatura de la generación filial «regresara» a la talla media de la población.

El término «regresión estadística» con que Galton publicara su trabajo se ha generalizado y hoy, sin sentido lingüístico alguno, se aplica a todo tipo de estudio de esta clase.

De todas las posibles regresiones, nosotros abordaremos la lineal, es decir, aquellas distribuciones bivariantes susceptibles de ser expresadas por una función lineal y, consecuentemente, representadas por una recta.

3.534. Ajuste. Método de los mínimos cuadráticos

Ajuste es el problema que consiste en determinar la función matemática que mejor represente una distribución bivariante aleatoria. No es cuestión que se pueda dejar al buen criterio del analista, pues, de este modo resultarían tantas *líneas de regresión* como apreciaciones subjetivas pudiera tener, a la hora de interpretar el diagrama de dispersión.

En primera aproximación, una simple inspección ocular de la nube de puntos permitirá escoger la forma de la línea que va a representar la regresión; convendrá, a este respecto, trazar una línea «provisional» que deje tantos puntos por arriba de ella, como por abajo.

Decidida la forma de la línea, por ejemplo, una recta, ha de resolverse el problema de calcular los parámetros de la recta que mejor represente la distribución. De todos los procedimientos para conseguirlo, el mejor, sin duda, es el que a continuación se desarrolla, bajo el título de

Método de ajuste por mínimos cuadráticos

Consiste este método en determinar los dos parámetros de la recta de regresión (su ordenada en el origen y su coeficiente angular), con la condición de que la suma de los cuadrados de las desviaciones entre los valores reales y los estimados sea mínima*. Es decir, siendo

$$d = y - y_e,$$

la condición descrita es

$$\Sigma d^2 = \text{mínima}.$$

* Con el fin de conseguir mayor agilidad de lectura, se suprimen en el desarrollo subsiguiente los *límites* de los sumatorios que se puedan suplir, sin ambigüedad.

Sea la recta de regresión

$$y_e = ax + b \qquad [25]$$

cuyos parámetros a y b se desean establecer por el método de los mínimos cuadráticos.

Según la condición de cálculo,

$$\Sigma(y - y_e)^2 = \Sigma(y - ax - b)^2 = \text{mínimo} \qquad [26]$$

Obsérvese que, para los efectos de nuestro cálculo, las variables de [26] son a y b.

Para determinar los valores que hacen mínima una función, es necesario que su derivada primera sea nula. En el caso que nos ocupa, por tener dos variables, a y b, han de ser nulas las derivadas primeras parciales, respecto de a y respecto de b.

$$\begin{aligned} \frac{d\Sigma}{db} &= \Sigma\, 2(y - ax - b)(-1) = 2\,\Sigma\,(-y + ax + b) = 0 \\ \frac{d\Sigma}{da} &= \Sigma\, 2(y - ax - b)(-x) = 2\,\Sigma\,(-xy + ax^2 + bx) = 0 \end{aligned} \qquad [27]$$

Desarrollando los sumatorios de [27] y dividiendo por 2, resulta:

$$\left.\begin{array}{ll} \text{I} & \Sigma y = Nb + a\Sigma x \\ \text{II} & \Sigma xy = b\Sigma x + a\Sigma x^2 \end{array}\right\} \qquad [28]$$

Las expresiones [28] constituyen las ecuaciones normales de la *recta de regresión de y sobre x*. Basta resolver el sistema, despejando a y b, para obtener la recta en su forma explícita.

$$y = \frac{\Sigma x \cdot \Sigma y - N\Sigma xy}{\Sigma^2 x - N\Sigma x^2} x + \frac{\Sigma y\, \Sigma x^2 - \Sigma x\, \Sigma xy}{N\Sigma x^2 - \Sigma^2 x}$$

Si en lugar de la recta $y_e = ax + b$, se trata de encontrar la recta $x_e = a'y + b'$, con la condición

$$\Sigma(x - x_e)^2 = \text{mínima},$$

se obtendrá una recta distinta de la anterior, denominada *recta de regresión de x sobre y*.

La razón de que ambas rectas no coincidan es precisamente que la dependencia es aleatoria y no funcional; en este último caso, ambas rectas se confundirían.

El cálculo para los parámetros a' y b' de esta recta de regresión de x sobre y es idéntico al anterior y con él se consiguen para la recta las siguientes ecuaciones normales

$$\begin{array}{ll} \text{I}' & \Sigma x = Nb' + a'\Sigma y \\ \text{II}' & \Sigma xy = b'\Sigma y + a'\Sigma y^2 \end{array} \qquad [29]$$

Tabla de datos y operaciones para el cálculo de las ecuaciones de regresión y coeficiente de correlación de la distribución (espesor, conductividad) de una serie de 100 piezas.

(x, y)	u_i / w_i	Espesor (x) mm													
		-4	-3	-2	-1	0	1	2	3	4	5	n_w	$n_w \cdot w_i$	$n_w \cdot w_i^2$	Σnuw
Conductividad (y) $\mu\Omega^{-1}$	-2	1 8	2 12	2 8								5	-10	20	28
	-1		3 9	8 16	9 9							20	-20	20	34
	0			1 0	10 0	32 0	10 0	5 0		2 0		60	0	0	0
	1				1 -1	1 0	6 6	2 4				10	10	10	9
	2						1 2	3 12			1 10	5	10	20	24
	n_u	1	5	11	20	33	17	10		2	1	100	-10	70	95
	$n_u \cdot u_i$	-4	-15	-22	-20	0	17	20		8	5	-11	$\sum$		
	$n_u \cdot u_i^2$	16	45	44	20	0	17	40		32	25	239			
	Σnuw	8	21	24	8	0	8	16		0	10	95			

NOTA. El número superior de cada casilla es la frecuencia de la clase bivariante respectiva; el inferior es el producto nu_iw_i.

A continuación se procede a realizar el ajuste y cálculo de ambas rectas de regresión, sobre el ejemplo (espesor, conductividad) de una serie de 100 piezas.

Advertencia. Conviene tener en cuenta que, con el fin de evitar notaciones farragosas, en la exposición precedente se han referido todos los cálculos, tácitamente, a una distribución de frecuencias no agrupadas.

Al aplicar a un ejemplo de frecuencias acumuladas las fórmulas deducidas, han de interpretarse los símbolos, que allí son referibles a individuos y que aquí han de referirse a clases. Así, cuando en [28] aparece Σy, ha de sustituirse -10, por ser la suma de las marcas de clase del segundo carácter (codificado w_i); o sea, ha de entenderse $\Sigma n_w w_i$; al aplicar el término Σxy, también en [28], ha de comprenderse que en frecuencias agrupadas toma la forma Σnuw (codificadas la x y la u y a w); si ha de calcularse Σx^2, adviértase que en frecuencias agrupadas se trata de $\Sigma n_u \cdot u_i^2$.

Con las advertencias precedentes, he aquí la tabla y cálculos.

Recta de regresión de y sobre x

$$\begin{array}{ll} \text{I} & -10 = 100b + a(-11) \\ \text{II} & 95 = b(-11) + a \cdot 239 \end{array}$$

$$a = 0{,}40 \qquad b = -0{,}058$$

Recta de regresión de x sobre y

$$\begin{array}{ll} \text{I} & -11 = 100b' + a'(-10) \\ \text{II} & 95 = b'(-10) + a' \cdot 70 \end{array}$$

$$a' = 1{,}36 \qquad b' = 0{,}02$$

Así pues, la recta de regresión de y sobre x tiene por ecuación

$$y_e = 0{,}40x - 0{,}058$$

y la de x sobre y es

$$y = \frac{1}{a'}x_e - \frac{b'}{a'} \; ; \quad y = 0{,}73x_e - 0{,}014$$

3.535. Cálculo abreviado de las rectas de regresión

Supuestas establecidas las dos rectas de regresión, hagamos una traslación de ejes a un nuevo origen $0'(\bar{x}, \bar{y})$ cuyas coordenadas son, precisamente, las medias de los dos caracteres de la variable, de modo que las coordenadas de un punto $P(x, y)$ respecto a los nuevos ejes serán $P(x', y')$

$$x' = x - \bar{x}$$
$$y' = y - \bar{y}$$

La recta de regresión de y sobre x, ahora tendrá por ecuación

$$y'_e = px' + q,$$

con la condición

$$\Sigma(y' - px' - q) = \text{mínima.}$$

Derivando como en 3.534 y reduciendo, se obtienen las ecuaciones

$$\left.\begin{aligned} \Sigma y' &= p\Sigma x' + N \cdot q \\ \Sigma x'y' &= p\Sigma x'^2 + q\Sigma x' \end{aligned}\right\} \qquad [30]$$

Pero $\Sigma x' = \Sigma y' = 0$, por ser sumas de las desviaciones respecto de la media, resultando entonces:

$$\left.\begin{aligned} q &= 0 \\ p &= \frac{\Sigma x'y'}{\Sigma x'^2} \end{aligned}\right\} \qquad [30']$$

El que sea $q = 0$ indica que la recta pasa por el nuevo origen, observándose además que su pendiente sigue siendo la misma.

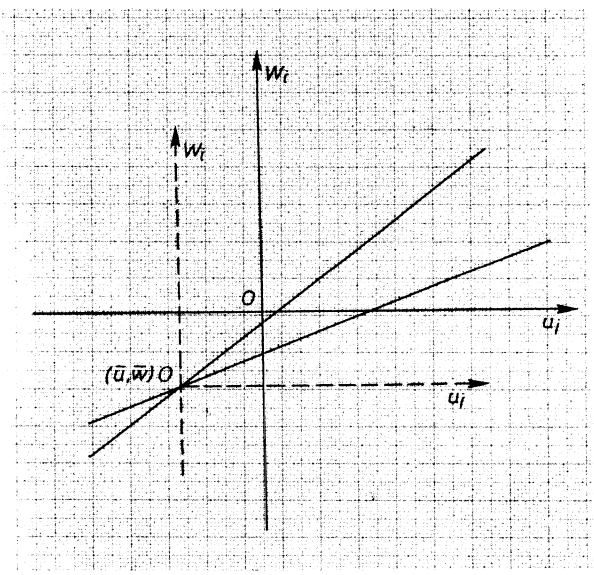
Un cálculo análogo para la recta de regresión de x sobre y, produce las ecuaciones

$$\left.\begin{aligned} q' &= 0 \\ p' &= \frac{\Sigma x'y'}{\Sigma y'^2} \end{aligned}\right\} \qquad [31]$$

Basta deshacer la traslación, si se desea, para obtener las rectas referidas a los primitivos ejes:

$$\begin{aligned} y_e - \bar{y} &= \frac{\Sigma x'y'}{\Sigma x'^2}(x - \bar{x}) \\ x_e - \bar{x} &= \frac{\Sigma x'y'}{\Sigma y'^2}(y - \bar{y}) \end{aligned} \qquad [32]$$

Finalmente, para cerrar este epígrafe, se representan las dos rectas de regresión del ejemplo que venimos desarrollando, y que han sido previamente calculadas.



3.536. Reducción de la información: estadísticos bivariantes. Correlación

Se denomina *correlación* a la relación de dependencia que existe entre los dos caracteres de una variable aleatoria.

Si al dibujar el diagrama de dispersión resultara que la nube de puntos representativos se encontraran todos sobre una línea, la dependencia no sería aleatoria, sino funcional, y su correlación sería «perfecta». En ese caso, las dos rectas de regresión coincidirían.

Si la nube de puntos denuncia, al dispersarse por todo el plano, la independencia total de los dos caracteres de la variable, al intentar dibujar las rectas de regresión se obtendrían una paralela al eje OX, para la regresión de y sobre x, y una aproximadamente paralela al eje OY, para la recta de regresión de x sobre y, resultando, en este caso, ambas rectas sensiblemente paralelas.

Entre los dos casos extremos establecidos, la mayor o menor dispersión de la nube de puntos dará lugar a que ambas rectas de regresión formen un ángulo entre sí, mayor o menor, también.

Es de suma importancia conseguir medir esa dependencia entre las dos variables de la distribución, y por lo que se lleva descrito, parece que el ángulo que forman entre sí las dos rectas de regresión sería una buena forma de cuantificar la correlación entre ambos caracteres. En efecto, se define:

Coeficiente de correlación lineal entre dos caracteres de una variable estadística bivariante es la media geométrica de los coeficientes a y a', de sus rectas de regresión.

$$r = \sqrt{a \cdot a'} \qquad [33]$$

Analicemos el comportamiento de la [33], en función de lo que pretende medir. Siendo a la pendiente de la recta de regresión de y sobre x y a', resultando ser la inversa de la pendiente de la recta de regresión de x sobre y, si por α y β se entienden las inclinaciones de las respectivas rectas, se tiene:

$$\left.\begin{aligned} a &= \operatorname{tg}\alpha \\ a' &= \frac{1}{\operatorname{tg}\beta} \end{aligned}\right\} \qquad [34]$$

y, entonces, sustituyendo [34] en [33], resulta:

$$r = \sqrt{\frac{\operatorname{tg}\alpha}{\operatorname{tg}\beta}}$$

Pero siendo siempre $\beta \geq \alpha$, sucede que $\dfrac{\operatorname{tg}\alpha}{\operatorname{tg}\beta} \leq 1$.

Queda así claro que el máximo valor de r es

$$\sqrt{r} = \sqrt{1} = \pm 1,$$

lo que sucederá cuando ambas rectas coincidan: se está frente a una dependencia funcional y la correlación entre las dos variables, entonces, es perfecta, lo que viene representado por el valor máximo de $r = 1$.

Por el contrario, si los dos caracteres de la variable bivariante resultan ser independientes, las dos rectas de regresión —como quedó dicho— son sensiblemente perpendiculares y entonces, $\alpha \simeq 0$ y $\beta \simeq 90°$. En este caso, el valor que toma r es

$$r = \sqrt{\frac{0}{\infty}} = 0$$

Así, pues, r se hace cero cuando la correlación es nula.

Puede ocurrir que α y β sean menores de 90°, con lo que sus tangentes son positivas. Se dice entonces que se trata de una *correlación directa y*, del signo doble de la raíz, se le asigna el positivo al coeficiente de correlación; si las inclinaciones de las rectas de regresión son mayores que 90°, ambas tangentes son negativas, y para denunciarlo se le asigna a r el signo menos de su raíz cuadrada: se dice, entonces, que se trata de un caso de *correlación inversa.*

El coeficiente de correlación y la desviación típica: covarianza.

Según se vio en [32]

$$a = \frac{\Sigma x'y'}{\Sigma x'^2} \quad \text{y} \quad a' = \frac{\Sigma x'y'}{\Sigma y'^2};$$

sustituyendo en [33],

$$r = \frac{\Sigma x'y'}{\sqrt{\Sigma x'^2 \cdot \Sigma y'^2}} \qquad [35]$$

Multiplicando y dividiendo el denominador por n, resulta:

$$r = \frac{\Sigma x'y'}{n\sqrt{\frac{\Sigma x'^2}{n} \cdot \frac{\Sigma y'^2}{n}}}$$

Recordando que $x' = x - \bar{x}$ y que $y' = y - \bar{y}$, se tiene:

$$r = \frac{\Sigma x'y'}{n \cdot \sigma_x \cdot \sigma_y} \qquad [36]$$

A $\dfrac{\Sigma x'y'}{n}$ se le denomina *covarianza*, por eso se puede enunciar que

> El coeficiente de correlación lineal es igual al cociente de la covarianza por el producto de las desviaciones típicas de cada una de las variables.

Cálculo del coeficiente de correlación

En la ecuación [35], sustituyendo la x' y la y' por lo que significan, resulta:

$$r = \frac{\Sigma(x - \bar{x})(y - \bar{y})}{\sqrt{\Sigma(x - \bar{x})^2 \cdot \Sigma(y - \bar{y})^2}}$$

Desarrollando los sumatorios,

$$r = \frac{\Sigma xy - \bar{y}\Sigma x - \bar{x}\Sigma y + n \cdot \bar{x}\bar{y}}{\sqrt{(\Sigma x^2 + n \cdot \bar{x}^2 - 2\bar{x}\Sigma x)(\Sigma y^2 + n \cdot \bar{y}^2 - 2\bar{y}\Sigma y)}}$$

Sustituyendo los valores medios por sus expresiones, se tiene:

$$r = \frac{\Sigma xy - \frac{\Sigma y}{n} \cdot \Sigma x - \frac{\Sigma x}{n} \cdot \Sigma y + n \cdot \frac{\Sigma x}{n} \cdot \frac{\Sigma y}{n}}{\sqrt{(\Sigma x^2 + n \cdot \frac{\Sigma^2 x}{n^2} - 2\frac{\Sigma x}{n} \cdot \Sigma x)(\Sigma y^2 + n \cdot \frac{\Sigma^2 y}{n^2} - 2\frac{\Sigma y}{n} \cdot \Sigma y)}};$$

operando,

$$r = \frac{\frac{1}{n}(n \cdot \Sigma xy - \Sigma x \cdot \Sigma y)}{\frac{1}{n}\sqrt{(n \cdot \Sigma x^2 - \Sigma^2 x)(n \cdot \Sigma y^2 - \Sigma^2 y)}};$$

finalmente,

$$r = \frac{n \cdot \Sigma xy - \Sigma x \cdot \Sigma y}{\sqrt{(n \cdot \Sigma x^2 - \Sigma^2 x)(n \cdot \Sigma y^2 - \Sigma^2 y)}} \qquad [37]$$

Si la muestra es muy extensa, se codifican las variables x e y a u y w y entonces, la [37] toma la forma

$$r = \frac{n \cdot \Sigma nuw - \Sigma n_u u_i - \Sigma n_w w_i}{\sqrt{(n\Sigma n_u u^2 - \Sigma^2 n_u u_i)(n\Sigma n_w w^2 - \Sigma^2 n_w w_i)}} \qquad [37']$$

Calculemos con [37'] el coeficiente de correlación de nuestra distribución bivariante (espesor, conductividad).

Todos los números recogidos se encuentran en la tabla de la página 416.

$$r = \frac{100 \times 95 - (-11) \times (-10)}{\sqrt{(100 \times 239 - (-11)^2)(100 \times 70 - (-10)^2)}} = 0{,}73$$

Puesto que se dispone de las pendientes de las rectas de regresión, se puede comprobar el cálculo, usando esas tangentes

$$r = \sqrt{\frac{\text{tg } \alpha}{\text{tg } \beta}} = \sqrt{\frac{0{,}40}{0{,}73}} = 0{,}74$$

3.54. DISTRIBUCIONES Y POBLACIONES ALEATORIAS

3.541. Introducción

La Estadística descriptiva es capaz de tratar con sus técnicas muestras finitas y dar un conocimiento completo de ellas. No sucede así en el caso de las poblaciones, pues su gran número de elementos prohíbe el análisis y toma de datos de todos y cada uno de sus individuos; entonces, la Estadística inferencial o teoría de muestras se encarga de escoger un subconjunto de esa población extensa, llamado muestra, que ha de ser aleatoria y representativa de toda la población. Se describe esa muestra y se infieren conclusiones para toda la población inaccesible.

Sin embargo, existen poblaciones naturales con un comportamiento específico que permiten, sin necesidad de la inferencia a partir de muestras, su descripción: son las llamadas *poblaciones aleatorias.*

Efectivamente, esas poblaciones aleatorias tienen la propiedad de que sus muestras presentan una distribución de frecuencias, tanto más parecidas a las llamadas *distribuciones probabilísticas o aleatorias*, cuanto más amplias se tomen. Resulta entonces que con una aproximación suficiente, para describir una población aleatoria, basta analizar la distribución aleatoria a que se asemeja. Como estas distribuciones son modelos rigurosamente teóricos cuyo análisis se puede realizar completo, al margen de todo empirismo, quiere decirse que la descripción estadística de las llamadas poblaciones aleatorias queda reducida al simple tratamiento matemático de esas distribuciones probabilísticas o aleatorias, que a continuación, se pasan a exponer.

3.542. Distribuciones aleatorias: función de distribución y función de densidad

Sea el espacio probabilístico $[P(H), p]$, formado sobre el muestral

$$H = \{H_1, H_2, \ldots H_n\}$$

Si a cada resultado se le asigna su probabilidad, queda establecida una función

$$\begin{aligned} P(H) &\xrightarrow{f} R \\ H_i &\longrightarrow f(H_i) = p_i \end{aligned} \qquad [38]$$

que se denomina *función de probabilidad.*

Se define, también, la *función de distribución* como

$$\begin{aligned} P(H) &\xrightarrow{f} R \\ H_i &\longrightarrow F(H_i) = p(H \leq H_i) \end{aligned} \qquad [39]$$

de modo que en ella la imagen de cada resultado H_i es igual a la probabilidad de que se verifiquen todos los resultados, menos o igual potentes que él.

En el caso de tratarse de variables aleatorias continuas, la función de probabilidad recibe el nombre de *función de densidad.*

Ejemplo

Sea la categoría de pruebas «lanzar dos dados sobre la mesa y computar los puntos conseguidos en sus caras superiores, en reposo».

El espacio muestral está constituido por los 36 resultados posibles

$$H = \{(1,1); (1,2); \ldots (1,6); \ldots (6,6)\}$$

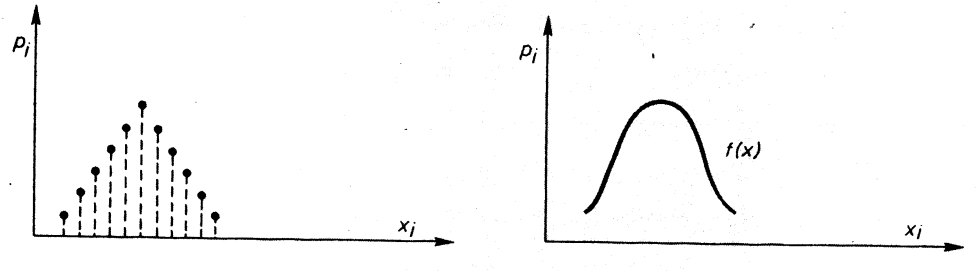
Se considera la función aleatoria que hace corresponder a cada suceso la suma de los puntos obtenidos. El conjunto de sus imágenes es

$$X = \{2, 3, 4, \ldots 11, 12\}$$

Sea ahora una función f sobre X, que asocia a cada resultado su probabiiidad *a priori*. He aquí su tabla de valores:

x_i	2	3	4	5	6	7	8	9	10	11	12
p_i	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

Se ha establecido la función de probabilidad de la variable aleatoria estudiada. Su representación, por tratarse de una variación discreta, dará lugar a un diagrama de puntos, en lugar de una línea continua, lo que sucedería de ser la variable aleatoria cuantitativa continua. del mismo tipo, con su diagrama de densidad.

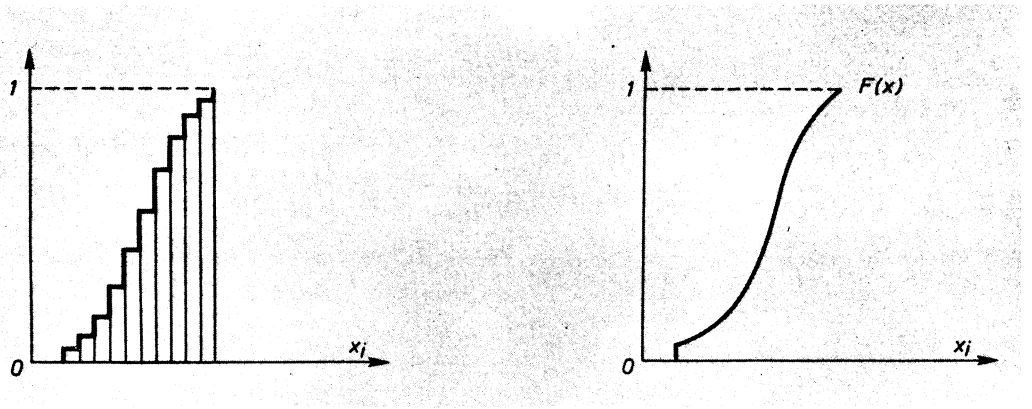


Tratemos ahora de establecer la función de distribución de esa variable aleatoria. El cuadro de valores es:

x_i	2	3	4	5	6	7	8	9	10	11	12
p_i ac.	$\frac{1}{36}$	$\frac{3}{36}$	$\frac{6}{36}$	$\frac{10}{36}$	$\frac{15}{36}$	$\frac{21}{36}$	$\frac{26}{36}$	$\frac{30}{36}$	$\frac{33}{36}$	$\frac{35}{36}$	1

y su representación da lugar a un diagrama acumulativo cuya ordenada máxima, lógicamente, siempre es 1 (véanse las figuras de la página siguiente).

Si se estuviera analizando una variable continua, de análogas características aleatorias, se habría conseguido una curva cuya forma sería el «límite» de la poligonal del diagrama.



3.543. Momentos de una distribución

La función de distribución de una variable estadística queda determinada por un conjunto de magnitudes que reciben el nombre de *momentos*. De todos ellos, sólo citaremos aquí tres: la esperanza matemática, media o valor esperado; la varianza y la desviación típica de la distribución.

Media o esperanza matemática

Sea x una variable aleatoria discreta que toma los valores

$$x_1, x_2, \ldots x_k$$

con las probabilidades correspondientes

$$p_1, p_2, \ldots p_k.$$

Se llama esperanza matemática de la distribución, que denotamos μ, el concepto que describe la siguiente fórmula:

$$\mu = \sum_{i=1}^{k} x_i p_i \qquad [40]$$

Intentando sensibilizar este momento, diremos que representa el valor que se puede esperar para la variable, como promedio de una elevada serie de ejecuciones.

La esperanza matemática o media del ejemplo anterior es

$$\mu = 2 \cdot \frac{1}{36} + 3 \cdot \frac{2}{36} + 4 \cdot \frac{3}{36} + \ldots + 12 \cdot \frac{1}{36} = 7$$

Varianza

Se establece como varianza de la distribución de una variable aleatoria discreta, denotada por σ^2, el momento que se formula

$$\sigma^2 = \sum_{i=1}^{k} (x_i - \mu)^2 \cdot p_i \qquad [41]$$

Desviación típica

En toda distribución aleatoria discreta, la desviación típica es igual a la raíz cuadrada positiva de su varianza

$$\sigma = \sqrt{\sum_{i=1}^{k} (x_i - \mu)^2 \cdot p_i} \qquad [42]$$

Compruébese, como ejercicio, que estos dos momentos, en el ejemplo que hemos establecido, valen, respectivamente

$$\sigma^2 = 35/6 \quad ; \quad \sigma = +\sqrt{35/6}$$

3.544. Distribución binomial

Recibe el nombre de distribución binominal la distribución de una variable aleatoria, tal que

a) sus clases son los resultados de la repetición indefinida de *n* pruebas aleatorias;
b) cada prueba puede dar lugar solamente a dos resultados;
c) las probabilidades de esos dos resultados son en todas las pruebas constantes.

La descripción del concepto que se acaba de escribir será convenientemente sustituida por la definición matemática del mismo, que suministra el análisis de una distribución binomial. Pero antes quede establecido un ejemplo, por demás típico, de una población cuya distribución se considera binomial*.

Ejemplo

Se lanza un número indefinido de veces, *n*, una moneda trucada al aire, de modo que la probabilidad de conseguir cara es 1/4 y la de obtener cruz, 3/4, en cada una de las pruebas.

Esta variable aleatoria presenta una distribución binomial.

Sea X una variable aleatoria con distribución binomial. Según ello, en cada prueba se pueden producir los sucesos excluyentes C o F, cuyas probabilidades se conocen *a priori*, y son

$$p(C) = p \quad ; \quad p(F) = q,$$

de modo que $p + q = 1$.

---

* Tal como aparece en el enunciado, es una distribución binomial, ya que se escribe «un número ilimitado de veces, *n*». Sucede que, realmente, no es posible ejecutar el proceso ilimitadamente; pero siendo *n* suficientemente grande, la aproximación es lícita.

Entendamos que se llevan a cabo n pruebas. Las clases de sucesos posibles son:

$$\begin{aligned}
H_n &= n \text{ veces } C \text{ y } 0 \text{ veces } F \\
H_{n-1} &= n-1 \text{ veces } C \text{ y } 1 \text{ vez } F \\
H_{n-2} &= n-2 \text{ veces } C \text{ y } 2 \text{ veces } F \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
H_i &= i \text{ veces } C \text{ y } n-i \text{ veces } F \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
H_0 &= 0 \text{ veces } C \text{ y } n \text{ veces } F
\end{aligned}$$

Analicemos cómo están constituidos cada uno de esos sucesos, sobre el genérico H_i:

1) H_i se puede presentar de $\binom{n}{i}$ formas distintas, que son las combinaciones de las n pruebas, tomadas de i en i, posibles secuencias de aparición del suceso C;
2) si se presenta una de esas formas de H_i no lo puede hacer simultáneamente otra de ellas, ya que son sucesos incompatibles;
3) cada una de esas formas, a su vez, está formada por la intersección de i sucesos C y $n-i$ sucesos F, independientes entre sí y, por tanto, la probabilidad de cada una de esas formas de presentarse H_i es el producto de las probabilidades de los i sucesos C y los $n-i$ sucesos F que las constituyen; es decir:

$$p(\text{forma}) = p^i \cdot q^{n-i};$$

4) como H_i está formado por la reunión de $\binom{n}{i}$ formas incompatibles, su probabilidad será la suma de las probabilidades de verificación de sus formas, de manera que

$$p(H_i) = \binom{n}{i} p^i q^{n-i} \qquad [43]$$

Con ello, ya se puede definir distribución binomial, diciendo que es la distribución que presenta una variable aleatoria, con la función de probabilidad establecida en [43].

Continuando con el ejemplo, se concreta sobre él lo establecido.

¿Cuál es la probabilidad de que al tirar seis veces la moneda trucada al aire se obtengan dos caras?

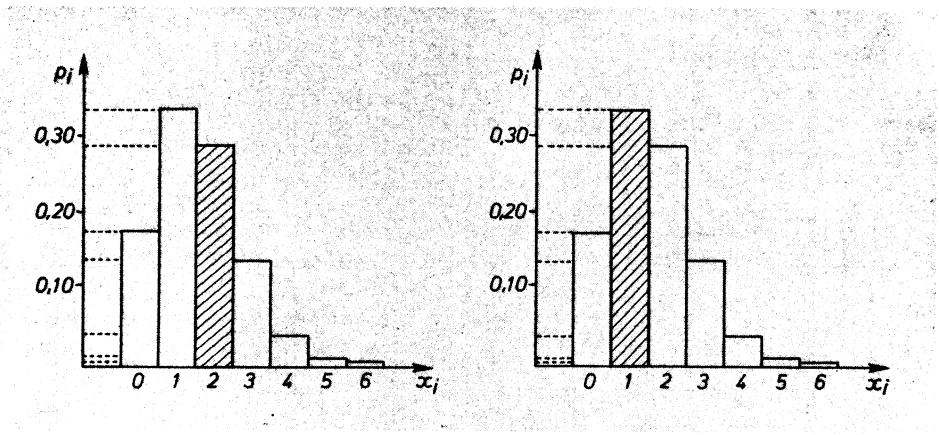
$$p = \frac{1}{4}; \quad q = \frac{3}{4}; \quad n = 6; \quad i = 2$$

$$p(2 \text{ caras}) = \binom{6}{2} \cdot \left(\frac{1}{4}\right)^2 \cdot \left(\frac{3}{4}\right)^4 = 0{,}29$$

¿Qué probabilidad hay de obtener cinco cruces?

$$i = 6 - 5 = 1$$

$$p(5 \text{ cruces}) = \binom{6}{1} \cdot \left(\frac{1}{4}\right)^1 \cdot \left(\frac{3}{4}\right)^5 = 0{,}353$$



En la ecuación [43], i puede tomar todos los valores comprendidos entre 0 y n, ambos inclusive, de modo que la distribución presenta $n + 1$ clases.

Ya es hora de advertir cuál es la razón del nombre: esta distribución se llama binomial porque su función de probabilidad, a lo largo de todo el espacio muestral, toma valores coincidentes con los términos del desarrollo del binomio de Newton $(p + q)^n$.

Cáigase en la cuenta de que, como $p + q = 1$, $(p + q)^n = 1^n = 1$.

Efectivamente, la

$$\sum_{i=0}^{n} \binom{n}{i} p^i \cdot q^{n-i} = 1,$$

que no es otra cosa que la probabilidad de todo el espacio muestral, a saber, el suceso seguro

$$p(H) = 1 = \sum_{i=0}^{n} \binom{n}{i} p^i \cdot q^{n-i} \qquad [44]$$

Son muy frecuentes las cuestiones en que ha de trabajarse con la función de distribución en lugar de con la función de probabilidad. Recuérdese que aquélla, definida en [39], se refería a probabilidades acumuladas. Un ejemplo aclara lo que se dice.

Ejemplo

Admitiendo que el engendrar hijos varones o mujeres son sucesos equiprobables, ¿cuál es la probabilidad de encontrar entre todas las familias con seis hijos, una que tenga 2, 3 ó 4 varones?

$$pr(\text{varón}) = p \quad ; \quad pr(\text{mujer}) = q$$

El problema, obviamente, se refiere a una distribución binominal de las siguientes características:

$$H = (4V \cap 2M) \cup (3V \cap 3M) \cup (2V \cap 4M)$$
$$p = q = 1/2$$
$$n = 6$$

La probabilidad de H es la suma de las probabilidades de los tres sucesos reunidos, incompatibles y, a su vez, cada uno de ellos, está formado por la intersección de los seis incompatibles y equiprobables que se indican, dentro de cada paréntesis.

Así, la probabilidad de H viene dada por la suma de los tres términos del desarrollo binomial que se escribe:

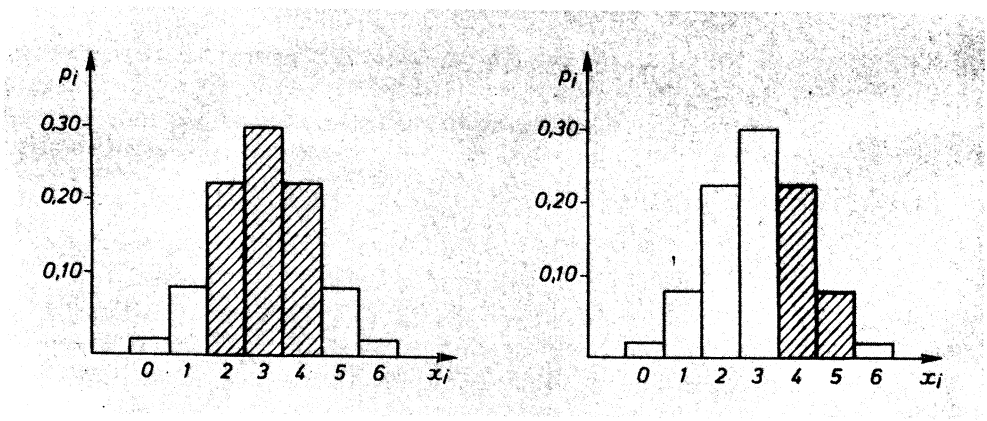
$$p(H) = \sum_{i=2}^{i=4} \binom{6}{i} \left(\frac{1}{2}\right)^i \cdot \left(\frac{1}{2}\right)^{6-i} = 0{,}781$$

Y, ¿cuál es la probabilidad de encontrar una de esas familias que tengan al menos cuatro varones?

$$H = (6V \cap 0M) \cup (5V \cap 1M) \cup (4V \cap 2M)$$

$$p(H) = \sum_{i=4}^{i=6} \binom{6}{i} \left(\frac{1}{2}\right)^i \cdot \left(\frac{1}{2}\right)^{6-i} = 0{,}345$$

En los diagramas, aparecen rayadas las áreas correspondientes.



Con el fin de evitar largos cálculos, se han construido tablas que dan, para distintos valores de n, p y q, los valores de los términos del desarrollo del binomio.

Para leer las que se facilitan, no se exigen mayores instrucciones.

Momentos

1) *Media.* Según [40], la esperanza matemática o media de una distribución aleatoria es

$$\mu = \sum_{i=1}^{k} x_i \cdot p_i$$

Basta sustituir en ella los límites específicos de la distribución discreta binomial, así como adaptar la simbología, para obtener

$$\mu = \sum_{i=0}^{n} x_i \cdot \binom{n}{i} \cdot p^i \cdot q^{n-i}$$

Un sencillo cálculo*, al desarrollar el número combinatorio, alcanza la expresión simplificada de la media, para estas distribuciones, que es

$$\mu = n \cdot p \qquad [45]$$

2) *Varianza y desviación típica.* A partir de la ecuación [41], se calcula que la varianza para una distribución binomial es

$$\sigma^2 = n \cdot p \cdot q \qquad [46]$$

resultando, entonces, para la desviación típica la expresión

$$\sigma = +\sqrt{n \cdot p \cdot q} \qquad [47]$$

Ejemplo

Los momentos del ejemplo inmediatamente antes establecido son:

$$\mu = 6 \cdot \frac{1}{2} = 3;$$

$$\sigma^2 = 6 \cdot \frac{1}{2} \cdot \frac{1}{2} = 3/2 \quad ; \quad \sigma = +\sqrt{3/2}$$

---

* Adviértase que, a efectos de cálculo, el símbolo x_i y el i producen los mismos números.

DISTRIBUCION BINOMIAL

Valores hasta $n = 10$ de $\binom{n}{i} p \cdot (1-p)^{n-i}$, para distintos valores de p

		p									
n	i	0,05	0,10	0,15	0,20	0,25	0,30	0,35	0,40	0,45	0,50
1	0	0,9500	0,9000	0,8500	0,8000	0,7500	0,7000	0,6500	0,6000	0,5500	0,5000
	1	0,0500	0,1000	0,1500	0,2000	0,2500	0,3000	0,3500	0,4000	0,4500	0,5000
2	0	0,9025	0,7100	0,7225	0,6400	0,5625	0,4900	0,4225	0,3600	0,3025	0,2500
	1	0,0950	0,1800	0,2550	0,3200	0,3750	0,4200	0,4550	0,4800	0,4950	0,5000
	2	0,0025	0,0100	0,0225	0,0400	0,0625	0,0900	0,1225	0,1600	0,2025	0,2500
3	0	0,8574	0,7290	0,6141	0,5120	0,4219	0,3430	0,2746	0,2160	0,1664	0,1250
	1	0,1354	0,2430	0,3251	0,3840	0,4219	0,4410	0,4436	0,4320	0,4084	0,3750
	2	0,0071	0,0270	0,0574	0,0960	0,1406	0,1890	0,2389	0,2880	0,3341	0,3750
	3	0,0001	0,0010	0,0034	0,0080	0,0156	0,0270	0,0429	0,0640	0,0911	0,1250
4	0	0,8145	0,6561	0,5220	0,4096	0,3164	0,2401	0,1785	0,1296	0,0915	0,0625
	1	0,1715	0,2916	0,3685	0,4096	0,4219	0,4116	0,3845	0,3456	0,2995	0,2500
	2	0,0135	0,0486	0,0975	0,1536	0,2109	0,2646	0,3105	0,3456	0,3675	0,3750
	3	0,0005	0,0036	0,0115	0,0256	0,0469	0,0756	0,1115	0,1536	0,2005	0,2500
	4	0,0000	0,0001	0,0005	0,0016	0,0039	0,0081	0,0150	0,0256	0,0410	0,0625
5	0	0,7738	0,5905	0,4437	0,3277	0,2373	0,1681	0,1160	0,0778	0,0503	0,0312
	1	0,2036	0,3280	0,3915	0,4096	0,3955	0,3602	0,3124	0,2592	0,2059	0,1562
	2	0,0214	0,0729	0,1382	0,2048	0,2637	0,3087	0,3364	0,3456	0,3369	0,3125
	3	0,0011	0,0071	0,0244	0,0512	0,0879	0,1323	0,1811	0,2304	0,2757	0,3125
	4	0,0000	0,0004	0,0022	0,0064	0,0146	0,0284	0,0488	0,0768	0,1128	0,1562
	5	0,0000	0,0000	0,0001	0,0003	0,0010	0,0024	0,0053	0,0102	0,0185	0,0312
6	0	0,7351	0,5314	0,3771	0,2621	0,1780	0,1176	0,0754	0,0467	0,0277	0,0156
	1	0,2321	0,3543	0,3993	0,3932	0,3560	0,3025	0,2437	0,1868	0,1359	0,0938
	2	0,0305	0,0984	0,1762	0,2458	0,2966	0,3241	0,3280	0,3110	0,2780	0,2344
	3	0,0021	0,0146	0,0415	0,0819	0,1318	0,1852	0,2355	0,2765	0,3032	0,3125
	4	0,0001	0,0012	0,0055	0,0154	0,0330	0,0595	0,0951	0,1382	0,1861	0,2344
	5	0,0000	0,0001	0,0004	0,0015	0,0044	0,0102	0,0205	0,0369	0,0609	0,0938
	6	0,0000	0,0000	0,0000	0,0001	0,0002	0,0007	0,0018	0,0041	0,0083	0,0156
7	0	0,6983	0,4783	0,3206	0,2097	0,1335	0,0824	0,0490	0,0280	0,0152	0,0078
	1	0,2573	0,3720	0,3960	0,3670	0,3115	0,2471	0,1848	0,1306	0,0702	0,0547
	2	0,0406	0,1240	0,2097	0,2753	0,3115	0,3177	0,2985	0,2613	0,2140	0,1641
	3	0,0036	0,0230	0,0617	0,1147	0,1730	0,2269	0,2679	0,2903	0,2918	0,2734
	4	0,0002	0,0026	0,0109	0,0287	0,0577	0,0972	0,1442	0,1935	0,2388	0,2734
	5	0,0000	0,0002	0,0012	0,0043	0,0115	0,0250	0,0466	0,0774	0,1172	0,1641
	6	0,0000	0,0000	0,0001	0,0004	0,0013	0,0036	0,0084	0,0172	0,0320	0,0547
	7	0,0000	0,0000	0,0000	0,0001	0,0001	0,0002	0,0006	0,0016	0,0037	0,0078
8	0	0,6634	0,4305	0,2725	0,1678	0,1002	0,0576	0,0319	0,0168	0,0084	0,0039
	1	0,2793	0,3826	0,3847	0,3355	0,2670	0,1977	0,1373	0,0896	0,0548	0,0312
	2	0,0515	0,1488	0,2376	0,2936	0,3115	0,2065	0,2587	0,2090	0,1569	0,1094
	3	0,0054	0,0331	0,0839	0,1468	0,2076	0,2541	0,2786	0,2787	0,2568	0,2188
	4	0,0004	0,0046	0,0185	0,0459	0,0865	0,1361	0,1875	0,2322	0,2627	0,2734
	5	0,0000	0,0004	0,0026	0,0092	0,0231	0,0467	0,0808	0,1239	0,1719	0,2188
	6	0,0000	0,0000	0,0002	0,0011	0,0038	0,0100	0,0217	0,0413	0,0403	0,1094
	7	0,0000	0,0000	0,0000	0,0001	0,0004	0,0012	0,0033	0,0079	0,0164	0,0312
	8	0,0000	0,0000	0,0000	0,0000	0,0000	0,0001	0,0002	0,0007	0,0017	0,0039
9	0	0,6302	0,3874	0,2316	0,1342	0,0751	0,0404	0,0207	0,0101	0,0046	0,0020
	1	0,2985	0,3874	0,3679	0,3020	0,2253	0,1556	0,1004	0,0605	0,0339	0,0176
	2	0,0629	0,1722	0,2597	0,3020	0,3003	0,2668	0,2162	0,1612	0,1110	0,0703
	3	0,0077	0,0446	0,1069	0,1762	0,2336	0,2668	0,2716	0,2508	0,2119	0,1641
	4	0,0006	0,0074	0,0283	0,0661	0,1168	0,1715	0,2194	0,2508	0,2600	0,2461
	5	0,0000	0,0008	0,0050	0,0165	0,0389					
	6	0,0000	0,0001	0,0006	0,0028	0,0087					
	7	0,0000	0,0000	0,0000	0,0003	0,0012	0,0039	0,0098	0,0212	0,0407	0,0703
	8	0,0000	0,0000	0,0000	0,0000	0,0001	0,0004	0,0013	0,0035	0,0083	0,0176
	9	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0001	0,0003	0,0008	0,0020
10	0	0,5987	0,3487	0,1969	0,1074	0,0563	0,0282	0,0135	0,0060	0,0025	0,0010
	1	0,3151	0,3874	0,3474	0,2684	0,1877	0,1211	0,0725	0,0403	0,0207	0,0098
	2	0,0746	0,1937	0,2759	0,3020	0,2816	0,2335	0,1757	0,1209	0,0763	0,0439
	3	0,0105	0,0574	0,1298	0,2013	0,2503	0,2668	0,2522	0,2150	0,1665	0,1172
	4	0,0010	0,0112	0,0401	0,0881	0,1460	0,2001	0,2377	0,2508	0,2384	0,2051
	5	0,0001	0,0015	0,0085	0,0264	0,0584	0,1029	0,1536	0,2007	0,2340	0,2461
	6	0,0000	0,0001	0,0012	0,0055	0,0162	0,0368	0,0689	0,1115	0,1596	0,2051
	7	0,0000	0,0000	0,0001	0,0008	0,0031	0,0090	0,0212	0,0425	0,0746	0,1172
	8	0,0000	0,0000	0,0000	0,0001	0,0004	0,0014	0,0043	0,0106	0,0229	0,0439
	9	0,0000	0,0000	0,0000	0,0000	0,0000	0,0001	0,0005	0,0016	0,0042	0,0098
	10	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0001	0,0003	0,0010

3.545. Distribución normal

3.5451. *Establecimientos*

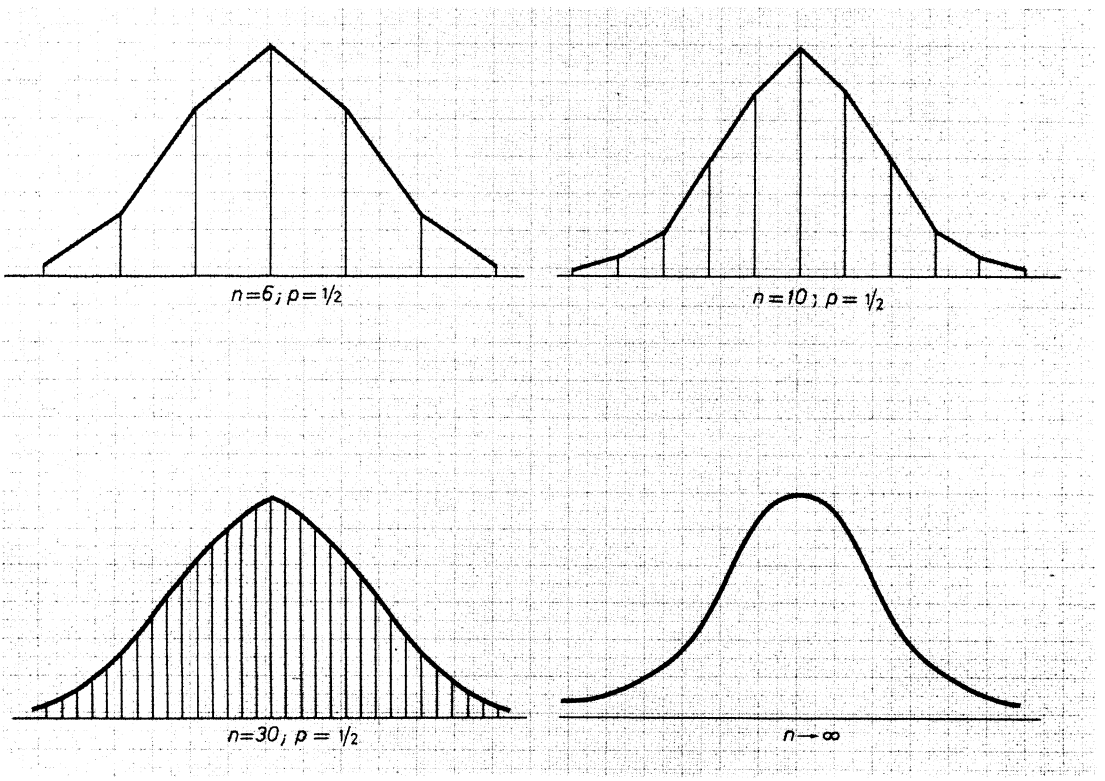
En 1773, De Moivre estableció la función de probabilidad que hoy se conoce con el nombre de distribución normal y cuya representación gráfica es la conocida «curva de Gauss o de campana».

Si en una distribución binomial sucede que p y q son números no muy diferentes, que $n \cdot p \geq 5$ y que la x_i aumenta ilimitadamente, al tiempo que lo hace n, resulta que su polígono de frecuencias es «suficientemente» parecido a la curva normal, cuya expresión analítica es

$$y = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \qquad [48]$$

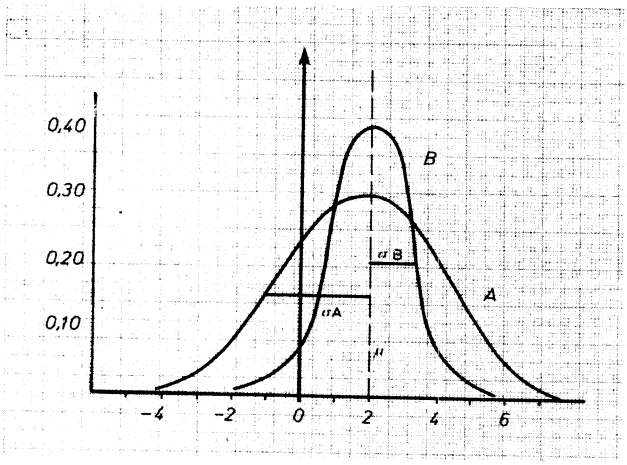
en la que σ y μ son la desviación típica y la media de la distribución.

Lo dicho queda de manifiesto en la figura múltiple adjunta.



Es frecuente denotar simbólicamente una distribución normal de media μ y desviación típica σ, escribiendo $N(\mu, \sigma)$.

La curva normal presenta las siguientes características:



Gráficas de dos distribuciones normales con media común, $\mu = 2$ y desviaciones típicas $\sigma_A = 3$ y $\sigma_B = 1{,}2$.

1. Las clases de distribución son puntuales y, por tanto, infinitas, como lo es n.
2. La curva normal es doblemente asintótica con el eje de abscisas.
3. El intervalo total o recorrido de la variable es limitado.
4. La función posee un máximo que se corresponde con los valores coincidentes de la moda, mediana y media.
5. La curva es simétrica, respecto de la ordenada del máximo.
6. La función posee dos puntos de inflexión simétricos, respecto a la ordenada media.
7. La desviación típica viene medida por el segmento $x_I - x_\mu$, diferencia de abscisas de una inflexión y la media.
8. Su coeficiente de asimetría es nulo, como corresponde a la forma de la curva.

Como consecuencia de 1), adviértase que no tiene sentido alguno asignar a la ordenada de un punto el significado de probabilidad de esa clase puntual. En una distribución normal sólo es posible determinar probabilidades de intervalos de valores de la variable aleatoria, y vienen representadas por las áreas parciales, encerradas por la curva, el eje de abscisas y las ordenadas levantadas por los límites del intervalo considerado.

La función de densidad $f(x)$ no representa probabilidades, pero el producto $f(x) \cdot \Delta x$ resulta ser aproximadamente igual a la probabilidad de que la variable tome un valor del intervalo $(x, x + \Delta x)$, de modo que se establece*:

$$p(a \leq x_i \leq b) = \int_a^b f(x)\, dx \qquad [49]$$

* Resulta inevitable establecer la integral. Para aquellos lectores, desconocedores del más elemental cálculo, puede ayudarles pensar en que si se tratara de una variable discreta, la probabilidad expresada sería

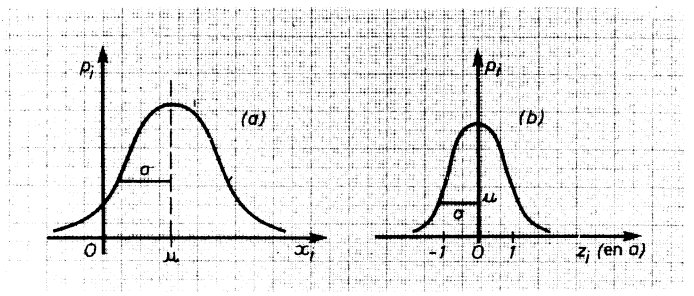
$$p(a \leq x_i \leq b) = \sum_{x_i = a}^{x_i = b} p(x_i),$$

de acuerdo con la naturaleza del cálculo: un número finito de sumandos. Cuando al ser la variación continua, el número de sumandos es ilimitado, el sumatorio se convierte en una integral definida, que es precisamente eso: una suma indicada de infinitos sumandos (infinito no numerable).

3.5452. *Tipificación de la variable. Tablas z/A*

Sea la distribución normal que se representa en *a*), $N(\mu, \sigma)$. Si en [48] se realiza el siguiente cambio de variable

$$z = \frac{x - \mu}{\sigma}$$



se obtiene una forma de la ecuación muy cómoda, referible a una distribución normal $N(0, 1)$, de media nula y desviación típica unidad (*b*).

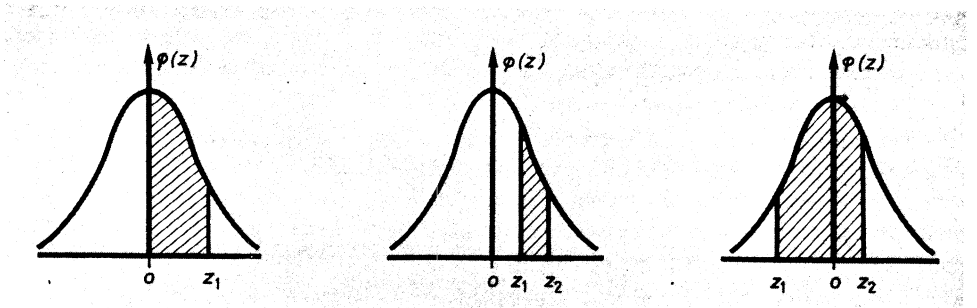
Así, la ecuación [48] toma la forma más simple

$$\varphi(z) = \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{1}{2}z^2} \qquad [50]$$

Una distribución tipificada ya no aparece descrita en milímetros, micras o cualquiera otra unidad en la que lo estuviera la distribución primitiva, sino que está descrita en desviaciones de cada valor a la media, medidas en desviaciones típicas. Consecuencia inmediata de ello es que si la desviación típica de la distribución primitiva fuera menor que la unidad, entonces la tipificación presenta una distribución más dispersa; y más agrupada alrededor de la media, en caso contrario.

Con el fin de evitar los engorrosos cálculos para la determinación de esas áreas limitadas por la curva normal, que fijan las probabilidades de que la variable tome un valor de un determinado intervalo, se han construido tablas que coleccionan valores de esas áreas para un buen número de valores de la tipificada z. De este modo, una sencilla resta entre los valores tabulados consigue la probabilidad del intervalo buscado.

Efectivamente, el cálculo de las probabilidades representadas en cada uno de los dibujos de la figura, son los que van a sus pies.



$p(0 \leq z \leq z_1) = Z_1$

$p(z_1 \leq z \leq z_2) = p(0 \leq z \leq z_2) - p(0 \leq z \leq z_1) = Z_2 - Z_1$

$p(z_1 \leq z \leq z_2) = p(0 \leq z \leq z_2) + p(0 \leq z \leq z_1) = Z_2 + Z_1$

Ejemplo

En una distribución $N(50, 5)$ determínese la probabilidad de que la variable tome valores comprendidos entre 32 y 40.

Primero habrá de tipificarse la variable x:

$$z = \frac{x - 50}{5}$$

$x_1 = 32 \Rightarrow z_1 = -3{,}6$
$x_2 = 40 \Rightarrow z_2 = -2$
$p(32 \leq x \leq 40) = p(-3{,}6 \leq z \leq -2) =$
$= p(-3{,}6 \leq z \leq 0) - p(-2 \leq z \leq 0) =$
$= 0{,}4998 - 0{,}4772 = 0{,}0226$

3.546. La distribución normal como aproximación de la binomial. Corrección de Yates

Si en una distribución binomial p o q no son demasiado próximos a cero y son tales que $np \geq 5$, $nq \geq 5$, con n suficientemente grande, las áreas limitadas por su histograma de frecuencias son sensiblemente coincidentes con las que determina la curva de campana de la distribución normal asociada a ella.

Si esto es así, en lugar de sumar las áreas dadas por el cálculo del binomio, se pueden computar aproximadamente por las tabuladas para la distribución normal correspondiente.

En efecto, el ejemplo que sigue especifica la técnica, aproximación y correcciones.

Ejemplo

¿Qué probabilidad hay de extraer una muestra de 10 bolas, formada por 3, 4 ó 5 negras y las restantes blancas, de una urna que contiene 1 000 bolas blancas y 1 000 bolas negras?

La probabilidad de obtener bola negra es $p = 1/2$ y la probabilidad de conseguir bola blanca es $q = 1/2$, de modo que la distribución binominal da:

$$p(H_i) = \sum_{i=3}^{i=5} \binom{10}{i} \left(\frac{1}{2}\right)^i \cdot \left(\frac{1}{2}\right)^{10-i}$$

$$p(H_i) = 0{,}56835$$

Si se considera la distribución como normal, ha de adecuarse la variación discreta de la variable a la continuidad de la variación normal. Por eso, los valores discretos 5 y 3 del carácter «número de bolas negras» ha de corregirse a los valores medios de sus correspondientes rectángulos del histograma, dando 5,5 y 3,5. Es la llamada *corrección de Yates.*

Se procede ahora a la tipificación de la variable:

$$x_1 = 2{,}5 \Rightarrow z_1 = \frac{2{,}5 - \mu}{\sigma} = -1{,}57$$

$$x_2 = 5{,}5 \Rightarrow z_2 = \frac{5{,}5 - \mu}{\sigma} = 0{,}31,$$

siendo $\mu = n \cdot p = 5$ y $\sigma = \sqrt{npq} = 1{,}58$.

Se dispone la lectura sobre las tablas de áreas

$$p(3 \leq x_i \leq 5) = p(-1{,}57 \leq z_i \leq 0{,}31) = p(0 \leq z_i \leq 1{,}57) + p(0 \leq z_i \leq 0{,}31) \quad ;$$

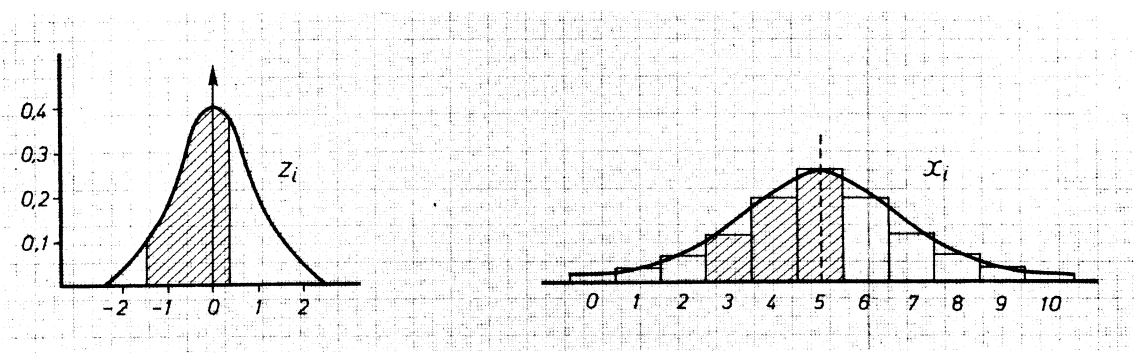
resultando:

$$p(H_i) = 0{,}4418 + 0{,}1217 = 0{,}5635.$$

Si se comparan los resultados habidos por el cálculo binomial y el normal, se observará una aproximación razonable, en la mayoría de los casos, válida.

La figura facilita la interpretación gráfica de esta aproximación.

El valor de n en el ejemplo es 10. La aproximación resulta tanto más fina cuanto más elevado sea n.

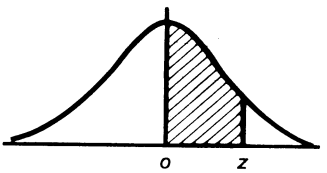


3.547. Distribución de Poisson

Desde que Quetelet describió «sus 100.000 soldados» en función de su talla y halló que éstas constituían una población normal, estableciendo la hipótesis de que el estudio estadístico de cualquiera otro carácter presentaría también distribución normal, se ha embalsamado, a nivel de principiantes, el error, puesto que tal hipótesis es falsa: ciertamente, gran número de caracteres forman pobla-

Areas limitadas en una curva normal tipificada entre el eje de las ordenadas y las ordenadas levantadas por distintos valores de z.

(De *Statistics*, por M. R. SPIEGEL. Schaum Publishing Company. Nueva York, 1961.)



z	0	1	2	3	4	5	6	7	8	9
0,0	0,0000	0,0040	0,0080	0,0120	0,0160	0,0199	0,0239	0,0279	0,0319	0,0359
0,1	0,0398	0,0438	0,0478	0,0517	0,0557	0,0596	0,0636	0,0675	0,0714	0,0754
0,2	0,0793	0,0832	0,0871	0,0910	0,0948	0,0987	0,1026	0,1064	0,1103	0,1141
0,3	0,1179	0,1217	0,1255	0,1293	0,1331	0,1368	0,1406	0,1443	0,1480	0,1517
0,4	0,1554	0,1592	0,1628	0,1664	0,1700	0,1736	0,1772	0,1808	0,1844	0,1879
0,5	0,1915	0,1950	0,1985	0,2019	0,2054	0,2088	0,2123	0,2157	0,2190	0,2224
0,6	0,2258	0,2291	0,2324	0,2357	0,2389	0,2422	0,2454	0,2486	0,2518	0,2549
0,7	0,2580	0,2612	0,2642	0,2673	0,2704	0,2734	0,2764	0,2794	0,2823	0,2852
0,8	0,2881	0,2910	0,2939	0,2967	0,2996	0,3023	0,3051	0,3078	0,3106	0,3133
0,9	0,3159	0,3186	0,3212	0,3238	0,3264	0,3289	0,3315	0,3340	0,3365	0,3389
1,0	0,3413	0,3438	0,3461	0,3485	0,3508	0,3531	0,3554	0,3577	0,3599	0,3621
1,1	0,3643	0,3665	0,3686	0,3708	0,3729	0,3749	0,3770	0,3790	0,3810	0,3830
1,2	0,3849	0,3869	0,3888	0,3907	0,3925	0,3944	0,3962	0,3980	0,3997	0,4015
1,3	0,4032	0,4039	0,4066	0,4082	0,4099	0,4115	0,4131	0,4147	0,4162	0,4177
1,4	0,4192	0,4207	0,4222	0,4236	0,4251	0,4265	0,4279	0,4292	0,4306	0,4319
1,5	0,4332	0,4345	0,4357	0,4370	0,4382	0,4394	0,4406	0,4418	0,4429	0,4441
1,6	0,4452	0,4463	0,4474	0,4484	0,4495	0,4505	0,4515	0,4525	0,4535	0,4545
1,7	0,4554	045,64	0,4573	0,4582	0,4591	0,4599	0,4608	0,4616	0,4625	0,4633
1,8	0,4641	0,4649	0,4656	0,4664	0,4671	0,4678	0,4686	0,4693	0,4699	0,4706
1,9	0,4713	0,4719	0,4726	0,4732	0,4738	0,4744	0,4750	0,4756	0,4761	0,4767
2,0	0,4772	0,4778	0,4783	0,4788	0,4793	0,4798	0,4803	0,4808	0,4812	0,4817
2,1	0,4821	0,4826	0,4830	0,4834	0,4838	0,4842	0,4846	0,4850	0,4854	0,4857
2,2	0,4861	0,4864	0,4868	0,4871	0,4875	0,4878	0,4881	0,4884	0,4887	0,4890
2,3	0,4893	0,4896	0,4898	0,4901	0,4904	0,4906	0,4909	0,4911	0,4913	0,4916
2,4	0,4918	0,4920	0,4922	0,4925	0,4927	0,4929	0,4931	0,4932	0,4934	0,4936
2,5	0,4938	0,4940	0,4941	0,4943	0,4945	0,4946	0,4948	0,4949	0,4951	0,4952
2,6	0,4953	0,4955	0,4956	0,4957	0,4959	0,4960	0,4961	0,4962	0,4963	0,4964
2,7	0,4965	0,4966	0,4967	0,4968	0,4969	0,4970	0,4971	0,4972	0,4973	0,4974
2,8	0,4974	0,4975	0,4976	0,4977	0,4977	0,4978	0,4979	0,4979	0,4980	0,4981
2,9	0,4981	0,4982	0,4982	0,4983	0,4984	0,4984	0,4985	0,4985	0,4986	0,4986
3,0	0,4987	0,4987	0,4987	0,4988	0,4988	0,4989	0,4989	0,4989	0,4990	0,4990
3,1	0,4990	0,4991	0,4991	0,4991	0,4992	0,4992	0,4992	0,4992	0,4993	0,4993
3,2	0,4993	0,4993	0,4994	0,4994	0,4994	0,4994	0,4994	0,4995	0,4995	0,4995
3,3	0,4995	0,4995	0,4995	0,4996	0,4996	0,4996	0,4996	0,4996	0,4996	0,4997
3,4	0,4997	0,4997	0,4997	0,4997	0,4997	0,4997	0,4997	0,4997	0,4997	0,4998
3,5	0,4998	0,4998	0,4998	0,4998	0,4998	0,4998	0,4998	0,4998	0,4998	0,4998
3,6	0,4998	0,4998	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999
3,7	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999
3,8	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999	0,4999
3,9	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000

ciones normales; pero no son pocos los que quedan lejos de la distribución de la curva de Gauss.

Tal sucede con la llamada distribución de Poisson.

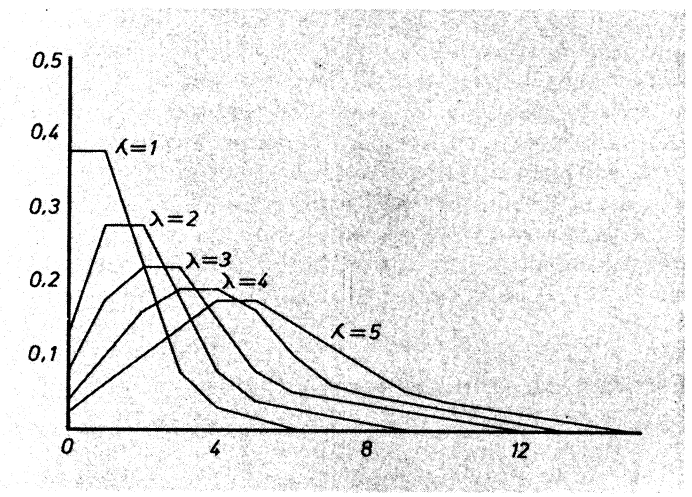
Consiste esta distribución en una variación binomial, cuando, permaneciendo x_i fijo, n tiende a infinito y p lo hace a cero, siendo $\lambda = np < 5$ constante.

En estas condiciones, la función de probabilidad es

$$y = p(x_i) = \frac{\lambda^i \cdot e^{-\lambda}}{i!} \qquad [51]$$

La [51] es una función discreta, con $\lambda > 0$.

En la figura adjunta se representan varias distribuciones de Poisson, para diversos valores de $\lambda = np$.



Obsérvese cómo, a medida que λ aumenta, la distribución de Poisson se acerca cada vez más a la forma normal.

Siendo $q \simeq 1$, los momentos de la distribución de Poisson, coinciden con los de la distribución binomial

$$\lambda = n \cdot p$$
$$\sigma = \sqrt{n \cdot p \cdot q} \simeq \sqrt{n \cdot p} = \sqrt{\lambda}$$

Ejemplo

Se admite que el número de hombres hemofílicos encontrados en muestras amplias es de 0,1 ‰.

¿Qué proporción de muestras aleatorias de 10.000 hombres cada una contendrán tres o cuatro enfermos?

Siendo $p = 0{,}0001$, se trata de una población superponible a una distribución de Poisson.

$$\lambda = n \cdot p = 10.000 \times 0{,}0001 = 1$$

$$p = \frac{1^3 \cdot e^{-1}}{3!} + \frac{1^4 \cdot e^{-1}}{4!} = 0{,}07$$

3.55. ESTADISTICA INFERENCIAL

3.551. Concepto. Clasificación

Para realizar el estudio estadístico de una población, la mayor parte de las veces no resulta posible tomar los datos a todos sus individuos, y esto por dos razones: bien porque la extensión de la población resulte prácticamente inabordable, bien porque el experimento a realizar en la medida sea destructivo. Piénsese, por ejemplo, en la imposibilidad de tomar todos los datos para realizar un estudio sobre el peso de la población mundial; compréndase lo prohibitivo del estudio total en el análisis estadístico de la resistencia a la rotura de una determinada pieza, fabricada en serie: si se rompen todas las piezas a analizar, se destruye la población.

La Estadística inferencial aborda este problema en sus dos partes: la Estadística inferencial inductiva y la Estadística inferencial hipotético-deductiva, también llamada teoría de la decisión.

3.552. Estadística inferencial inductiva

El objetivo de esta ciencia es doble:

1) el desarrollo de técnicas que permitan *estimar* los parámetros de una población, a partir de los estadísticos de una muestra representativa y aleatoria de la misma;
2) medir la incertidumbre de la inducción.

La muestra escogida para hacer el estudio descriptivo ha de ser un subconjunto de la población *representativo* y *aleatorio*;

a) *Muestra representativa.* La composición de la muestra ha de ser análoga a la composición de la población que intenta representar. No es válido tomar un subconjunto del que se sospecha que la distribución del carácter en sus individuos ocupa un extremo de la distribución de la población.
b) *Muestra aleatoria.* Con frecuencia, resulta difícil conseguir una muestra que, siendo representativa, sea a la vez aleatoria. De cualquier modo, es tarea que corresponde a otra disciplina íntimamente ligada a la Estadística, pero distinta de ella: el diseño de experimentos.

Dispuesta la muestra representativa y aleatoria, se procede a su descripción y determinación de sus estadísticos; calculados éstos, se realiza la tarea de la in-

ferencia inductiva, propiamente dicha: la estimación de los parámetros de la población.

Esta estimación puede realizarse «puntualmente», fijando un valor del parámetro que se estima, o «por intervalo», calculando dos valores que sean extremos del intervalo, dentro del cual se estima que se encuentra el parámetro buscado.

Resulta más conveniente la estimación por intervalo que la puntual, porque de aquel modo se consigue, de paso, fijar la incertidumbre de la estimación en probabilidades fiduciales.

3.553. Estadística inferencial hipotético-deductiva

El objetivo de esta parte de la teoría de muestras es desarrollar la técnica apropiada para comprobar hipótesis sobre los parámetros de una población y para medir en probabilidades fiduciales la incertidumbre de la misma.

Se conoce con el nombre de *test estadístico* la técnica seguida para aceptar o rechazar un parámetro desconocido de una población, en función de los estadísticos calculados de una muestra de ella.

El método a seguir para la comprobación de una hipótesis estadística consta de las siguientes fases:

1.ª *Enunciación* de la hipótesis de trabajo, H_0, en términos de parámetros y estadísticos;

2.ª *Deducción* de conclusiones, en términos de distribución muestral. Para ello han de hacerse dos cosas:

- 2*a*) Fijar el estadístico muestral, relacionado con el parámetro de la hipótesis; y
- 2*b*) determinar la *región crítica* o *de rechazo*, que es el intervalo de la distribución muestral que contendría un bajo porcentaje llamado *nivel de significación*, de valores grandes y/o pequeños de la distribución, en caso de que el parámetro de la población a que se refiere la hipótesis tuviera, en efecto, el valor que se le supone.

  Suelen ser niveles de significación corrientes el 1 por 100 o el 5 por 100.

  La diferencia entre el intervalo total de la distribución y la región crítica se denomina *zona de aceptación.*

  Si la región crítica sólo contiene valores grandes o valores pequeños de la variable, la comprobación suele llamarse *unilateral*; si la zona de rechazo está formada por los dos extremos de la distribución, se dice, entonces, que la comprobación es *bilateral.*

3.ª *Verificación* de conclusiones. Consiste en tomar la muestra y calcular sobre ella los estadísticos a que se refiere la hipótesis.

4.ª *Decisión.* Se trata de aceptar la hipótesis o rechazarla, según las siguientes normas:

- 4*a*) si el estadístico calculado pertenece a la región crítica, la hipótesis se rechaza, ya que la probabilidad de obtener un valor como el probado es del orden del nivel de significación adoptado; 0,1 ó 0,5, generalmente; como se ve, baja. Y ello no se considera atribuible a un error de muestreo. Se considera que las conclusiones no han sido confirmadas;
- 4*b*) si, por el contrario, el estadístico calculado queda en la zona de acep-

tación, se admite la hipótesis como correcta, con una medida de certidumbre que viene fijada, precisamente, por el nivel de significación. He aquí un ejemplo, con el que se cierra esta breve noticia de la inferencia estadística:

Ejemplo

Un suero A resulta efectivo frente a una determinada infección en un 25 por 100 de los casos. Un nuevo suero B se ensaya en fase clínica, observándose que de 10 tratamientos han resultado con éxito 8.

¿Es suficiente esta fase de la investigación para decidir que el suero B es igual o más efectivo que el A?

Hipótesis de trabajo: Igual efectividad de ambos sueros

$$H_0 \begin{cases} \text{probabilidad de éxito: } p(+) = 0{,}25 \\ \text{probabilidad de fracaso: } p(-) = 0{,}75 \end{cases}$$

La distribución de las medias de las infinitas muestras de extensión 10, se tabulan en el cuadro siguiente:

$\bar{x}$	0	1/10	2/10	3/10	4/10	5/10	6/10	7/10	8/10	9/10	1
$p(+)=0{,}25$	0,0563	0,1877	0,2816	0,2503	0,1460	0,0584	0,0162	0,0031	0.0004	0.0000	0.0000

Se fija el nivel de significación en el 1 por 100.

La muestra (10 tratamientos/8 éxitos) ha de ser de media $\bar{x} = 8/10$.

Comprobemos si, en efecto, es compatible con la hipótesis H_0:

$$p(\bar{x} \geq 8/10) = 0{,}0004 + 0{,}0000 + 0{,}0000 = 0{,}0004$$

Ha resultado, pues, que el 0,04 por 100 de las muestras de lo tratamientos resultarían con una media igual o superior a la exigida por la hipótesis.

El resultado cae en la zona crítica. La decisión es clara: se rechaza la hipótesis, ya que el suceso a que da lugar la muestra tratada es «raro» en la distribución.

3.56. APLICABILIDAD. AUTOMATISMOS Y DESTREZAS

3.560.

Tabule y represéntense de todos los modos posibles la población de alumnos de su curso, en función de las asignaturas optativas que cursan.

3.561.

Se facilita el cuadro de observaciones referibles al grado de acidez de 100 muestras, formadas en serie, de un determinado catalizador. Establézcase la tabla de frecuencias agrupadas en diez intervalos.

3.562.

Dibújese el histograma de frecuencias, el polígono de frecuencias y el polígono acumulativo de la distribución anterior.

pH									
5,40	5,49	5,49	5,52	5,49	5,58	5,64	5,67	5,73	5,76
5,70	5,73	5,76	5,70	5,76	5,67	5,64	5,79	5,91	5,82
5,79	5,85	5,88	5,85	5,79	5,91	5,94	6,06	5,94	5,91
6,06	5,79	5,85	5,85	5,79	5,91	5,92	5,95	5,88	5,88
6,03	5,97	5,97	6,00	6,00	6,03	6,03	5,97	5,94	6,00
6,00	6,00	5,97	6,06	6,06	6,03	5,97	6,06	5,94	6,03
6,09	6,00	5,94	5,94	6,03	5,94	5,94	5,97	6,06	6,00
6,12	6,21	6,12	6,12	6,15	6,21	6,18	6,15	6,12	6,09
6,16	6,12	6,15	6,21	6,18	6,15	6,18	6,24	6,36	6,36
5,79	6,24	6,27	6,27	6,30	6,33	6,33	6,54	6,66	6,81

3.563.

Determínese la moda y mediana de esa población.

3.564.

Calcúlese su recorrido intercuartílico y sus desviaciones medias.

3.565.

Codificada la variable a u_i, tabúlese y calcúlese la media y la desviación típica de la distribución.

3.566.

Compruébese que tipificando la variable a z_i, la media es nula y la desviación típica 1.

3.567.

La actividad catalítica de las cien muestras anteriormente tabuladas se ha medido en microgramos de sustrato transformado por unidad de tiempo de reacción, resultando las 100 masas siguientes:

m									
7,70	7,80	7,75	7,80	7,75	7,82	7,80	7,85	7,80	7,85
7,80	7,85	7,85	7,90	7,85	7,90	7,80	7,90	7,90	7,90
7,85	8,00	7,85	7,98	7,90	7,92	7,90	8,00	7,90	7,95
8,00	8,00	7,90	8,00	7,92	7,80	7,90	8,00	8,00	7,95
8,00	8,10	7,95	8,10	8,00	8,00	8,00	8,00	7,95	8,00
7,90	8,00	7,95	8,15	8,00	8,00	7,98	8,10	7,95	8,05
8,04	8,15	7,90	8,00	8,00	8,00	7,90	8,00	8,00	8,00
8,05	8,20	8,00	8,10	8,05	8,10	8,05	8,10	8,05	8,10
8,08	8,06	8,05	8,15	8,06	8,10	8,05	8,12	8,10	8,20
7,85	8,12	8,10	8,15	8,10	8,18	8,08	8,15	8,25	8,40

Hágase el estudio completo de la regresión (pH/m), estableciendo ambas líneas de regresión.

3.568.

Calcúlese el coeficiente de correlación de la distribución bivariante anterior.

3.569.

Admitiendo que en la ciudad A, durante el mes de agosto la temperatura diurna oscila siguiendo una distribución normal, siendo la media de 38° y la desviación típica 8°, ¿qué probabilidad hay de que el termómetro marque 39° ó 40°?

3.6

Teoría de la Información

3.61. Introducción

3.62. La noción de información. Unidad de información

3.63. Entropía de un suceso aleatorio

3.631. *Concepto*
3.632. *Una propiedad de la entropía*

3.64. Un ejemplo de aplicación

3.65. Ordenadores

3.651. *Máquinas de calcular. Antecedentes históricos*
3.652. *Tipos de máquinas calculadoras. Ordenadores*
3.653. *Elementos de un ordenador*
3.654. *Breve idea del funcionamiento de un ordenador*

3.6

Teoría de la información

3.61. INTRODUCCION

Una de las cosas que ha permitido llegar al hombre al grado de cultura y civilización actual, al desarrollo de la ciencia y al dominio de la técnica que hoy disfrutamos (?), es, sin duda, su capacidad para recibir, almacenar y transmitir información.

Ciertamente esa capacidad no es privativa del ser humano, sino que es extensiva a todo ser vivo. Es la característica fundamental de la vida: la perpetuación generacional de las especies no es más que un proceso dirigido por la información genética que cada individuo-hijo recibe de sus progenitores, que, a su vez, él almacena durante su vida en la «despensa cromosómica» y transmite a su descendencia.

Lo característico de la especie humana es que, aparte de esta información esencial, ha sido capaz de desarrollar, en primer lugar, un sistema de comunicación para transmitir información, la palabra, y, en una segunda etapa, un sistema de almacenamiento de la misma, la escritura.

Todos los demás avances posteriores (imprenta, telefonía, registros electromagnéticos, etc.) han permitido mayor difusión, rapidez de transmisión o velocidad superior de acceso a una determinada información, pero no han aportado nada nuevo al esquema básico de

transmisión-recepción-almacenamiento

de la información.

En lo que se lleva escrito se ha utilizado el término «información» en el sentido con el que se maneja comúnmente. Pero en cuanto se trate de esquematizar desde un punto de vista matemático todo lo que de matematizable tiene la información, nos veremos obligados —como en tantas otras ocasiones— a descargar el término de todo el contenido no esencial, quedándonos de un modo preciso y neto con su esencia. Por ello, el primer objetivo ha de ser contestar a esta pregunta: ¿Qué es la información?

3.62. LA NOCION DE INFORMACION. UNIDAD DE INFORMACION

Siempre que se recibe una información, en el sentido usual de la palabra, se entiende que, de un universo más o menos grande de posibilidades (los posibles mensajes), se ha seleccionado una, la que se recibe.

La información viene a deshacer una indeterminación, y parece lógico pensar que la información recibida es tanto mayor cuanto mayor fuera en principio la indeterminación.

Indeterminación e información se encuentran así ligadas de modo natural entre sí y a los sucesos aleatorios, cuya característica principal es la incertidumbre de su resultado antes de su verificación.

Sea A un suceso aleatorio cuyos posibles resultados, en número finito, se designan

$$a_1, a_2, \ldots, a_n,$$

y cuyas probabilidades respectivas son

$$p(a_1), p(a_2), \ldots, p(a_n).$$

Asociado con este suceso, siempre hay un grado de indeterminación, y «se intuye» que diferentes sucesos han de tener distintos grados de indeterminación, aun cuando no se sepa evaluarlos con cierta garantía de objetividad.

Ejemplo

Considérense dos cajas iguales, contenedoras, la primera, de noventa y nueve bolas blancas y una negra; la segunda, de cincuenta blancas y cincuenta negras.

Sea la experiencia que consiste en extraer una bola de la primera caja; considérese también el experimento de sacar una bola de la segunda caja.

La impresión que se tiene, previa a la ejecución de las pruebas, es que el primer experimento es «más determinado» que el segundo en la obtención de bola blanca. Se está «casi seguro» de obtener bola blanca, aun cuando no se descarte la posibilidad de sacar bola negra.

Nuestro objetivo es, pues, definir una función de las probabilidades $p(a_i)$ que mida el grado de indeterminación de un suceso aleatorio y que permita comparar dos sucesos, en lo que a indeterminación se refiere; es decir, obtener una función que dé una medida objetiva de lo que subjetivamente se percibía en el ejemplo precedente.

Comencemos por el caso en que todos los resultados de A son equiprobables:

$$p(a_i) = 1/n \qquad i = 1, 2, \ldots, n$$

La función que se pretende definir (que aquí tendrá como única variable, n) va a obedecer a las siguientes condiciones:

1.ª $S(1) = 0$.
2.ª Si $n_1 < n_2$, entonces $S(n_1) < S(n_2)$.
3.ª $S(m \cdot n) = S(m) + S(n)$.

Consecuencia inmediata de la primera y segunda condiciones es

$$S(n) \geq 0.$$

Aun cuando así conformadas, las condiciones establecidas parecen del todo arbitrarias, tienen una razón de ser que intentamos explicar, viendo cómo recogen tres exigencias fundamentales que ha de pedirse a la función que trata de medir la indeterminación del suceso aleatorio A.

La primera condición responde al hecho de que si $n = 1$, es decir, si el suceso A tiene un solo resultado posible, la indeterminación es nula, ya que el resultado se conoce antes de realizarse la experiencia.

La segunda condición es referible a que entre dos sucesos aleatorios con resultados equiprobables, debe ser más indeterminado aquel que tiene mayor número de posibles resultados.

En cuanto a la tercera, si se consideran dos sucesos aleatorios A y B, *independientes*, con n y m resultados equiprobables, respectivamente, establecido el suceso intersección $A \cdot B$, que tiene $n \cdot m$ resultados posibles, también equiprobables, tal suceso compuesto es más indeterminado que cualquiera de los dos A o B, pues a la indeterminación del uno se le añade la del otro. Parece lógico, pues, establecer que la indeterminación del suceso compuesto es la suma de las indeterminaciones de los que le componen. Siempre, se insiste, en el supuesto que sean sucesos independientes.

Una función que cumple las tres condiciones impuestas es la función

$$S(n) = \log n,$$

con la única limitación de que la base del sistema de logaritmos sea mayor que la unidad. Adviértase que si la base fuera un número entre 0 y 1, no se cumpliría la segunda condición.

Por otra parte, la elección de la base es arbitraria, ya que el cambio de base supone sólo multiplicar por una constante, es decir, a fin de cuentas, cambiar de unidad de medida de la indeterminación.

Si se toma como base el número 2, entonces, resulta una unidad llamada unidad binaria o *bit*:

> *Bit* es la indeterminación de un suceso aleatorio con dos resultados equiprobables.

3.63. ENTROPIA DE UN SUCESO ALEATORIO

3.631. Concepto

Hasta ahora se han considerado únicamente sucesos aleatorios con resultados equiprobables.

Para extender la medida del grado de indeterminación a otro tipo cualquiera de sucesos aleatorios, partamos de considerar los resultados equiprobables del suceso A, anteriormente establecido:

$$a_1, a_2, \ldots, a_n.$$

La indeterminación de A es $\log_2 n$.

Cada uno de los n resultados posibles introduce una indeterminación igual a $(\log_2 n)/n$, siendo la indeterminación total la suma de todas esas indeterminaciones parciales.

Teniendo en cuenta que $\log_2 n = -\log_2 \frac{1}{n}$, se puede escribir:

$$\log_2 n = -\frac{1}{n} \log_2 \frac{1}{n} = -p(a_i) \log_2 p(a_i),$$

donde $p(a_i)$ representa la probabilidad del resultado a_i, ya que en el caso de resultados equiprobables

$$p(a_i) = 1/n, \quad \text{para todo } i.$$

La relación anterior permite definir ahora el grado de indeterminación total de un suceso aleatorio A con resultados no necesariamente equiprobables

$$a_1, a_2, \ldots, a_n,$$

con probabilidades respectivas, no necesariamente iguales

$$p(a_1), p(a_2), \ldots, p(a_n).$$

$$S|p(a_1), p(a_2), \ldots, p(a_n)| = -\sum_{i=1}^{n} p(a_i) \log_2 p(a_i)$$

La función S, así definida, se denomina *entropía* del suceso aleatorio A.

Considérese, de nuevo, un suceso aleatorio A con n resultados equiprobables. Como se ha visto anteriormente, el grado de indeterminación de tal suceso es $\log_2 n$, de manera que la elección de un resultado entre los n suministra una información igual a la indeterminación que elimina, a saber: $\log_2 n$.

De otro modo: si se recibe un mensaje seleccionado de entre n igualmente probables, la información recibida es $\log_2 n$.

Obsérvese que

$$\log_2 n = -\log_2 (1/n) = -\log p(a_i),$$

en el caso de que todas las probabilidades sean iguales.

Según esto, al considerar un suceso aleatorio cualquiera, podríamos sentirnos inclinados a decir que la información obtenida al producirse el resultado a_i es $-\log_2 p(a_i)$, con lo que diferentes resultados darían distintas informaciones.

Ejemplo

Se considera el experimento aleatorio, consistente en extraer de una bolsa que contiene cinco bolas blancas y una negra, una bola y constatar su color.

Los dos posibles resultados son: bola blanca;
bola negra.

Las probabilidades respectivas son: $p(B) = 5/6$;
$p(N) = 1/6$.

Si se obtiene bola blanca, la información recibida es $-\log_2 (5/6) = \log_2 (6/5)$, mientras que si la extracción produce bola negra, la información obtenida es $-\log_2 (1/6) = \log_2 S$, claramente superior, lo que está de acuerdo con la idea intuitiva que se tiene de la información:

Cuanto más probable es un resultado, tanta menos información da el hecho de su verificación, pues, de principio, se está «casi seguro» de su realización.

Por esta razón, la medida de la información, *asociada a un resultado*, de un experimento o suceso aleatorio, que acabamos de dar no es la que se utiliza; en su lugar, se considera la información media de todos los posibles resultados, afectados cada uno de su probabilidad. Es decir, se toma como medida de la información la cantidad

$$\boxed{\sum_{i=1}^{n} p(a_i)|-\log_2 p(a_i)| = -\sum_{i=1}^{n} p(a_i)\log_2 (a_i)},$$

que no es más que la entropía del suceso aleatorio.

Continuando con el ejemplo anterior, la información media o entropía del suceso vale

$$S(5/6,\ 1/6) = -\frac{5}{6}\log_2 \frac{5}{6} - \log_2 \frac{1}{6} = 0{,}6865$$

3.632. Una propiedad de la entropía

Considérese un suceso aleatorio con sólo dos posibles resultados, a_1 y a_2. Sus probabilidades son

$$p(a_1) = p \quad ; \quad p(a_2) = 1 - p.$$

La entropía alcanza el valor

$$S(p) = -p \log p - (1 - p)\log (1 - p).$$

Demostraremos que la entropía es máxima cuando $p = 1 - p = 1/2$.

En efecto: La función $S(p)$, completada en los puntos 0 y 1, definiendo $S(0) = 0$ y $S(1) = 0$, es continua en $|0, 1|$ y positiva en $(0, 1)$ y, por anularse en los extremos del intervalo, cualquier máximo relativo en ese intervalo lo será absoluto. Teniendo en cuenta que

$$S'(p) = -\log p + \log (1 - p) = \log \frac{1 - d}{p},$$

la anulación de la derivada corresponde a $\frac{1 - p}{p} = 1$, o sea,

$$1 - p = p,$$

con lo que

$$p = 1/2.$$

Se puede demostrar que en el caso de n resultados con probabilidades $p(a_1), \ldots, p(a_n)$, la entropía es máxima cuando $p(a_1) = p(a_2) = \cdots = p(a_n)$. No demostraremos esta proposición, pero haremos uso de ella.

3.64. UN EJEMPLO DE APLICACION

Consideremos un problema sencillo, que ilustra suficientemente todo lo que se lleva establecido.

Supóngase que se pide el menor número de preguntas, a contestar sí o no, necesarias para determinar completamente un número natural menor o igual que 1 000 que se ha pensado.

El número de resultados posibles es 1 000, todos igualmente probables (el número a determinar puede ser uno cualquiera entre 1 y 1 000, ambos inclusive).

La indeterminación es, pues,

$$\log 1\,000 = 9{,}9658 \textit{ bits}$$

Cada pregunta, como puede tener sólo dos respuestas posibles, a lo sumo nos dará una información de 1 bit. Se necesitan entonces un mínimo de diez preguntas para determinar el número pensado. Con menos, no será posible; pero cabe que hubieran de utilizarse más, si no se sabe sacar el máximo de información de cada pregunta realizada.

Por ejemplo, una manera poco ventajosa de preguntar sería formular una pregunta del tipo

«¿El número pensado es el número 15?»

La probabilidad de que la pregunta sea contestada con un sí es 1/1 000 y 999/1 000 es la de que sea contestada con un no. La información recibida de este modo es

$$-\frac{1}{1\,000} \log \frac{1}{1\,000} - \frac{999}{1\,000} \log \frac{999}{1\,000} = 0{,}0114 \text{ bits.}$$

Como puede comprenderse, muy lejos del máximo de 1 bit que podría haberse obtenido.

La explicación es clara, pues al formular la pregunta, las posibles respuestas no eran equiprobables, condición necesaria para que la entropía y, por tanto la información recibida, sea máxima.

Esto marca la pauta para hacer la pregunta más ventajosa. Una pregunta del tipo

«¿El número pensado es menor o igual que 500?»,

da una igual probabilidad de ser respondida sí o no, con lo que la información obtenida será, exactamente,

$$-\frac{1}{2}\log\frac{1}{2}-\frac{1}{2}\log\frac{1}{2}=1 \text{ bit.}$$

El resto de las preguntas con la misma tónica, lleva en diez preguntas al número pensado.

3.65. ORDENADORES

3.651. Máquinas de calcular. Antecedentes históricos

En los apartados anteriores hemos estudiado la noción de información. El desarrollo espectacular de la Astronáutica y del aprovechamiento de la energía nuclear, el impulso dado en los diversos campos de la investigación, etc., han sido posibles por el rápido desarrollo de los medios de obtener información.

Una vez obtenida la información, se impone manipularla para obtener resultados aplicables a soluciones de problemas, a decisiones que se han de tomar, a estudiar características del conjunto de una población, etc.

La información viene expresada en la gran mayoría de los casos por medio de números, y su manipulación consiste en la obtención de nuevos números a partir de los datos. El hombre ha tenido que seleccionar la forma de obtener los nuevos números para que sean significativos del conocimiento que buscamos de la información, así como los datos numéricos que deben constituir la información de partida.

La obtención de la información que constituyen los datos numéricos del problema, y asimismo su manipulación para obtener nueva información, puede resultar, y lo es en la mayoría de los casos, un trabajo rutinario, pesado, aburrido. Gracias al empleo de las modernas máquinas calculadoras, conocidas con el nombre de «calculadores electrónicos», el hombre ha podido liberarse de ese trabajo puramente mecánico para dedicar su atención a trabajos intelectuales de interpretación de resultados y selección de datos de entrada.

Las máquinas calculadoras electrónicas se denominan «Ordenadores» (del francés «Ordinateur»); también se utiliza el nombre más largo «Sistema de pro-

ceso de datos» (del inglés «Data Processing System»). Utilizaremos la primera denominación que es más breve. Asimismo se usa indistintamente la palabra «Computador», puesto que su finalidad es el cómputo o cálculo.

Desde los tiempos más antiguos el hombre ha intentado buscar ayudas mecánicas que faciliten el cálculo. En este orden de ideas aparecieron históricamente los ábacos, la regla de cálculo y las máquinas de calcular.

Los ábacos, constituidos por bolas ensartadas en alambres, existen desde hace más de dos mil quinientos años. No hay que confundir los ábacos como rudimentaria máquina de representar y sumar números por medio de bolas, basándose en el principio del valor de posición de las bolas o valor relativo, con los gráficos que se utilizan para cálculos en laboratorios, oficinas técnicas, etc., y que por extensión se les da el mismo nombre.

La *regla de cálculo* es la materialización mecánica de unas tablas de logaritmos. Su antigüedad puede admitirse, coincidiendo con la aparición de los logaritmos, hace unos trescientos cincuenta años. Con este ingenioso y sencillo mecanismo se obtiene menos precisión que con las tablas logarítmicas, pero resulta suficiente en la mayoría de los casos y se gana enormemente en rapidez.

La máquina de calcular tiene su origen en el mecanismo creado por Blas Pascal, en 1642, al sustituir las bolas enfiladas en varillas del tradicional ábaco por ruedas giratorias en cuya circunferencia están las cifras de 0 a 9. El perfeccionamiento sobre el ábaco consistió en «contar las unidades que se llevan» automáticamente, cosa que no se podía hacer con el ábaco.

El matemático inglés Charles Babbage concibió en 1833, o sea, dos siglos después de que Pascal realizara su máquina aritmética, una calculadora que fuese capaz de recibir no sólo los datos numéricos, sino también las *instrucciones* del trabajo a efectuar con dichos datos. Gastó su fortuna y su tiempo tratando de construirla, pero quedó en mero proyecto por dificultades tecnológicas.

El filósofo y matemático Leibniz (1646-1716), con su idea de un lenguaje lógico universal (*mathesis universalis*), preparó, desde el punto de vista especulativo, el *razonamiento automatizado*, base de los computadores.

Un siglo después de Babbage, hacia 1940, se construía en Estados Unidos la primera máquina calculadora moderna, el modelo MARK 1, por Howard Aiken.

En 1945, por obra del ingeniero eléctrico J. Eckert y del físico J. Mauchly se concluía la máquina ENIAC (Electronic Numerical Integrator and Computer) diseñada para una secuencia de cálculos muy específica, concretamente para calcular las tablas de disparo del Departamento de Artillería del Ejército.

El diseño de ENIAC fue estudiado por el matemático John von Neumann, quien quedó obsesionado por la idea de crear una máquina que tuviera un programa *flexible*. En 1952, gracias a la concepción de Neumann, se construyó el MANIACI (Mathematical Analyzer, Numerical Integrator and Computer), el primero que responde a la técnica actual.

3.652. Tipos de máquinas calculadoras. Ordenadores

Existen dos grandes grupos de máquinas calculadoras: analógicas y digitales.

En la calculadora analógica, los datos numéricos de entrada se representan mediante magnitudes físicas *continuas* (desplazamientos mecánicos, voltajes, etc.) y los resultados de la máquina se dan en forma semejante. Como ejemplo de

máquinas calculadoras analógicas tenemos la mayoría de los órganos de regulación en los procesos de fabricación industrial. También podemos citar la *regla de cálculo*.

En la calculadora digital, los datos numéricos se representan mediante señales que equivalen a cifras numéricas de un sistema de numeración adecuado (generalmente binario); es de carácter *discreto*.

Vamos a desarrollar breves consideraciones sobre las calculadoras digitales, que son las que admiten un lenguaje lógico-matemático.

La expresión más avanzada de una máquina calculadora digital la constituye el moderno *ordenador*, que se caracteriza por la facultad de poder tomar *decisiones lógicas*.

Se dice que una calculadora es capaz de tomar *decisiones lógicas* cuando puede cambiar la sucesión de operaciones que realiza en función de los resultados intermedios.

3.653. Elementos de un ordenador

Un ordenador consta de cinco unidades o elementos principales, que citamos a continuación:

Unidad de entrada

Por medio de esta unidad se suministra a la máquina la información siguiente:

- datos
- programa
  - operaciones
  - decisiones lógicas
  - resultados requeridos en la unidad de salida

Unidad de memoria

En esta unidad quedan localizados:

- datos
- instrucciones del programa
- resultados intermedios

En la memoria no sólo se localizan los datos, instrucciones y resultados intermedios de un problema concreto, sino que también nos sirve como un archivo de datos entre los cuales puede figurar el resultado de un cálculo anterior.

Unidad de control

Coordina las acciones de las distintas unidades funcionales. Decide qué orden han de seguir las operaciones, obedece las decisiones lógicas y transmite órdenes a los órganos de entrada y salida. Todo esto lo realiza de acuerdo con las instrucciones almacenadas en la memoria.

Unidad aritmética

En esta unidad se efectúan las operaciones aritméticas, adición, sustracción, multiplicación y división. Estas sencillas operaciones se reducen a las dos primeras, e incluso, a la primera. No descendemos a detalles que pueden encontrarse en cualquier tratado de computadores; lo que sí destacaremos es que cualesquiera operaciones, por ejemplo, la extracción de raíces, cálculo de funciones trigonométricas, etc., puede reducirse a las anteriores. Podemos decir brevemente, para que

se capte la idea: «el computador electrónico sólo sabe sumar y restar, pero tiene la ventaja de que lo hace a gran velocidad».

Unidad de salida

En esta unidad aparece el resultado del cálculo pedido al ordenador. Puede ocurrir que este resultado vaya a ser utilizado por otro ordenador, en cuyo caso conviene que venga expresado por medio de fichas perforadas, cintas magnéticas, etcétera. Cuando el hombre es el usuario directo del resultado suele venir impreso en caracteres ordinarios, que a veces acompañan a gráficas de puntos (meteorología, hidrografía, etc.).

3.654. Breve idea del funcionamiento de un ordenador

Vamos a razonar sobre modelos que no son los más modernos, pero que pueden servirnos para captar el principio de funcionamiento.

Si un número cualquiera se representa en el sistema de numeración binario, las únicas cifras de que constará serán 0 y 1. Cada uno de estos dígitos va a tener la denominación de *bit* («binary unit»), palabra que hemos usado anteriormente.

En una ficha de cartulina o en una cinta de papel, podemos representar las cifras 1 mediante orificios y las cifras 0 por medio de celdillas sin perforar. De esta manera puede quedar registrada en la cinta o ficha de cartulina cualquier información representada por una secuencia de cifras 0 ó 1, mediante perforaciones suficientemente espaciadas.

La ficha (o cinta) perforada es leída por la máquina en la unidad de entrada, de forma que, en correspondencia con cada espacio o unidad de información, existe un circuito que se cierra si corresponde a una perforación o queda abierto en caso contrario. De esta forma la perforación (dígito 1) se traduce en un impulso de corriente eléctrica, y la carencia de perforación (o dígito 0) se traduce en una ausencia de impulso.

El mecanismo de cierre del circuito se puede realizar por medio de escobillas sensibles que conectan a través de las perforaciones, o por células fotoeléctricas cuya radiación pasa a través del orificio. La idea siempre es la misma: el cierre del circuito eléctrico y el impulso correspondiente o la apertura del circuito con ausencia de impulso.

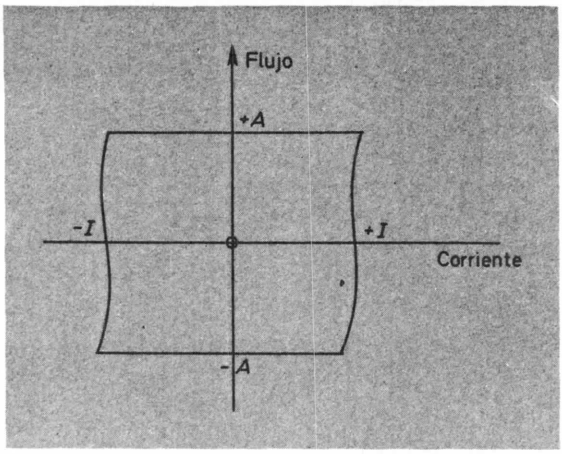
La información que la máquina lee en la unidad de entrada se registra en la memoria.

Vamos a considerar una memoria de núcleos de ferrita. Este es un material cuyo ciclo de histéresis es prácticamente un rectángulo.

Si se hace pasar una corriente, en la figura de la página siguiente, $+I$ deja el material en estado de magnetización $+A$, y si se hace pasar una corriente de sentido contrario $-I$ le hace alcanzar el estado $-A$. Podemos asignar a $+A$ el dígito 1 y a $-A$ el 0.

Los anillos cerámicos impregnados de ferrita (de diámetro poco mayor de 1 mm) quedan magnetizados con signo + o −, esto es, representan o almacenan los datos de la información introducida.

En vez de anillos de ferrita se emplean memorias de cinta y discos magnéticos. El principio es el mismo: sobre la cinta se encuentran celdillas magnéticas neutras que pueden magnetizarse positiva o negativamente por medio de un electroimán que recibe el impulso eléctrico en uno u otro sentido.



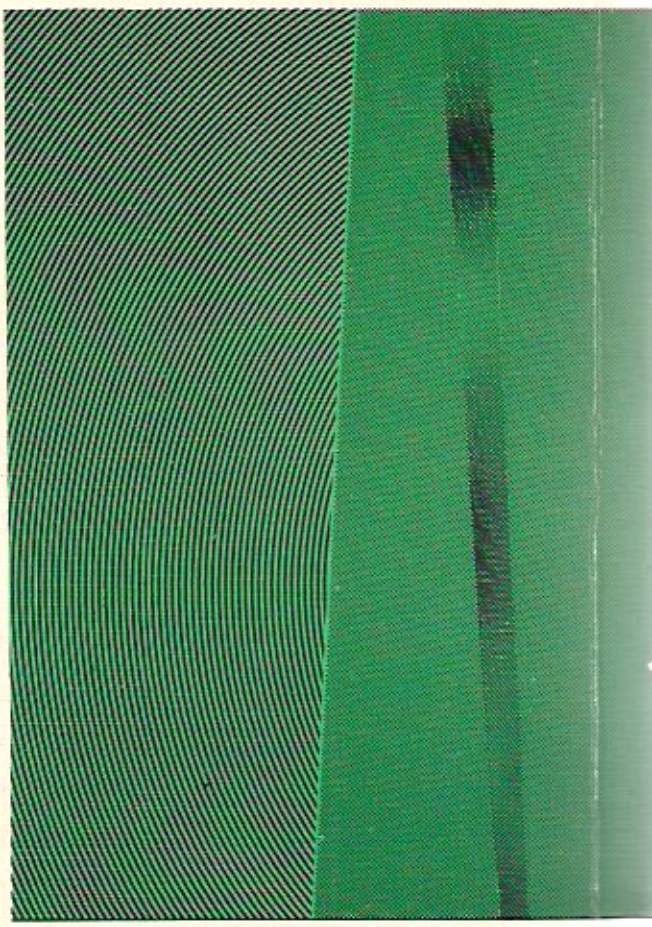
Existen otros procedimientos de memorizar, como mediante un tubo de rayos catódicos, diodos de vacío y condensador, diodos de germanio y transistores, que constituyen mejoras tecnológicas, pero la idea es la misma.

El proceso mediante el que pasa la información contenida en la memoria a la unidad de salida es análogo (basta invertir el sentido) al paso de la unidad de entrada a la memoria. Si se desea la impresión en la unidad de salida en caracteres tipográficos ordinarios (letras, números), existen varios procedimientos (impresión de barras verticales, de disco giratorio, etc.) que traducen los impulsos eléctricos en presión del correspondiente tipo de imprenta sobre el papel carbón que graba la hoja de resultados.

El orden de operaciones aritméticas, el cálculo de las mismas y las decisiones lógicas según los resultados intermedios, funciones propias de las unidades de control y aritmética, se realizan construyendo circuitos que materializan las operaciones. El principio es bastante simple, pero su construcción resulta laboriosa.

Los números 0, 1 pueden representar los dos resultados posibles de la lógica «no» «sí», luego los mismos símbolos que usamos para la representación de números sirven para establecer el valor lógico de las proposiciones, lo cual tiene la ventaja de la simplicidad y de la facilidad de mecanización de la aritmética binaria, como hemos visto, mediante fichas perforadas, material magnético y otros modos posibles.

Todas las instrucciones que se dan a un ordenador han de efectuarse en su propio lenguaje simbólico. No existe un lenguaje universal aplicable a cualquier ordenador; no obstante, hay dos, FORTRAN (FORmula TRANslation) y ALGOL (ALGOrithmic Language) que han tenido bastante aceptación; el primero es el lenguaje de la programación científico-técnica. Estos temas pueden verse en numerosos tratados especializados.

Dentro del esquema conciso que nos hemos propuesto al desarrollar estas ideas sobre la información y su elemento más representativo, el ordenador, sólo nos queda por decir que gracias al ordenador ha sido posible resolver cálculos que no cabía concebir, por ejemplo, resolver un sistema de cien ecuaciones lineales con cien incógnitas, que con el computador ATLAS (1964) se resolvería en quince segundos. Este simple ejemplo puede hacernos comprender el valor inmenso que tiene esta herramienta de la que el hombre dispone.

Alhambra
Ciencias y Técnica